REPORT

TABULATION UPGRADE SECURITY REVIEW & RISK ANALYSIS

Report prepared for:

KING COUNTY ELECTIONS

REPORT COMPLETED BY:

ANITIAN
ENTERPRISE SECURITY
888-ANITIAN ◆ WWW.ANITIAN.COM

ANITIAN
ENTERPRISE SECURITY

TABLE OF CONTENTS

ANITIAN
ENTERPRISE SECURITY

Project: Tabulation Upgrade Security Review & Threat Analysis
Deliverable Assessment Report
Revision 3.10
Client: King County Elections
Date: June 24, 2009

Document Revision History

Date	Number	Description of changes and purpose
3/3/2009	0.10	Initial Draft – Adam Gaydosh and Al Davidson
4/6/2009	0.20	Updates from new version testing – Adam Gaydosh
4/14/2009	0.30	Election Operational Processes and Procedures Analysis supplement and draft peer review – Al Davidson
4/17/2009	0.31	Style & Layout Changes – Andrew Plato
4/22/2009	0.40	Edits and enhancements – Adam Gaydosh
4/22/2009	0.41	Peer Review – Al Davidson
4/22/2009	0.42	Peer Review – Andrew Plato
5/9/2009	0.50	Edits made in response to last minute delivery and validation of technical information provide by PES – Adam Gaydosh
5/13/2009	0.51	Peer Review – Al Davidson
5/13/2009	0.52	Peer Review – Andrew Plato
5/14/2009	0.60	Additional content – Adam Gaydosh
5/14/2009	0.61	Final Editing – Andrew Plato
5/15/2009	0.62	Add Appendix, Final Edits – Adam Gaydosh
5/15/2009	1.00	First Final Draft
5/29/2009	1.10	Edits – Adam Gaydosh
5/31/2009	1.20	Layout changes and new text for Executive Summary – Andrew Plato
6/2/2009	1.30	Additional Material – Al Davidson
6/2/2009	1.40	Edits – Andrew Plato
6/2/2009	2.00	Second Final Draft Delivered to Customer – Adam Gaydosh
6/15/2009	2.10	Edits from 6/11/09 meeting – Adam Gaydosh
6/21/2009	2.20	Additional edits from 6/19/09 meeting – Adam Gaydosh
6/22/2009	3.00	Final Version – Andrew Plato
6/23/2009	3.10	Minor grammar and typographic edits – Andrew Plato

Contact Information

King County Personnel

Person	Role	Email	Phone
Bill Huennekens	Vote by Mail Transition Manager	Bill.Huennekens@kingcounty.gov	206.296.9932

Anitian Personnel

Person	Role	Email	Phone
Adam Gaydosh	Senior Security Analyst	adam.gaydosh@anitian.com	503.726.2116
Andrew Plato	Principal Security Consultant	andrew.plato@anitian.com	503.726.2117
Al Davidson	Elections Administration Expert	aldavidson-ems@comcast.net	503-930-9820

ANITIAN
ENTERPRISE SECURITY

1. INTRODUCTION

King County Elections (KCE) hired Anitian to conduct a security review and threat assessment of the Assure 1.2 voting system (Assure) from Premier Election Solutions (PES).

The overall goal of this project is to maintain public confidence in KCE's election systems through the systematic and objective identification and analysis of the technical and procedural risks that are relevant to the system.

1.1. Background

Pursuant to motion adopted by council 2007-0402, the threat assessment of the Premier Elections Solution (formerly Diebold) Assure 1.2 voting system shall be done within the parameters of the real world election environment in King County.

- The King County Elections Security Plan (page 3) states that:
  - Effective security does not rely on a single process, feature or policy. Effective security requires a number of interrelated process, systems and policies that complement and build on each other." The systems, process and policies that comprise layers of security for King County Elections (KCE).
- The Overview of the California Top To Bottom Review further illustrates this point:
  - "Security traditionally relies on layers of mechanisms; this is called *defense in depth*, *layered defens*e, or *separation of privilege*. The idea is to force an attacker to breach several security mechanisms to compromise the system, rather than one. Procedures form some of these layers of defensive mechanisms. Proper system configuration and implementation form additional layers of defensive mechanisms. Security plans should *always* rely on multiple layers."
  - "If a problem is discovered, the people who know the law and election policies and procedures can modify their policies and procedures appropriately to attempt to address a problem."
  - "Therefore, the results of this study must be evaluated in light of the context in which these systems are used. This emphasizes a Key point often overlooked in the discussion of the benefits and drawbacks of electronic voting systems: those systems are part of a process, the elections process; and the key question is whether the election process, taken as a whole, meets the requirements of an election as defined by the body politic."
  - "It is commonly accepted that no computer-based system, called an information technology system can be made completely secure."
- To protect against individuals that have greater access to the hardware and software, a system of defense that provide for a detection of inappropriate activity is critical. The systems employed need to provide this capability and Elections' procedures must implement and enforce this capability.

It is within this framework of King County Election's procedural and physical security that the security review threat assessment of the upgraded vote tabulation system in King County is to be evaluated; so that security concerns can be identified and associated risks mitigated so that voters can have trust and confidence in the voting system in King County.

1.2. Work Order

In December 2007, KCE issued a work order to companies that were qualified on their vendor roster to complete security assessments and analysis. Anitian responded to this work order and was awarded the contract to complete the assessment.

This work order contained the following requirements.

1. *Review the Independent Testing Authority reports from the federal certification process as a starting point for the threat assessment. Identify areas not covered by the federal process and review/test those areas*

2. *With understanding that the California Top To Bottom Review was done on an older version of the product suite; review the new suite and documentation to determine if issues identified in the California Top To Bottom Review with the TSx and GEMS equipment and systems have been mitigated in the new version of the solution suite and if not, if KCE procedures sufficiently protect against the remaining vulnerabilities*
3. *Review the report "Software Review and Security Analysis of the Diebold Voting machine Software" done for the Florida Department of State and examine if any of the flaws documented in the report have been mitigated by the newer version of the TSx software and if not, if KCE procedures sufficiently protect against remaining vulnerabilities.*
4. *Unless the contractor identifies areas they feel were not adequately addressed, the contractor is not to duplicate the efforts of the ITA, California TTBR, or Florida review. Before duplicating any effort, the contractor shall seek the concurrence of the county.*
5. *Employ voting system threat modeling by examining the inputs and outputs of the system to assist in determining the structure of the intrusion/penetration testing including but not limited to components numbers 6, 7, 8.*
6. *Intrusion or penetration testing of the ballot tabulation system*
   A. *Reviewers will conduct intrusion or penetration testing, of the functions and performance of the Premier Elections Solution Assure 1.2 voting system, to identify and document vulnerabilities, if any, to tampering or error that could cause incorrect recording, tabulation, tallying or reporting of votes or that could alter critical election data such as election definition or system audit data. This testing will be conducted in secured King County Elections' facilities.*

7. *In order to facilitate an understanding of the system its uses and functions the contractor shall provide a technician to be an operator as part of the tabulation team conducting the mock election and volume testing that are part of the acceptance testing process. The technician will be required to participate in the training conducted by the vendors and King County Elections.*
8. *Finally, the following specific security features or potential vulnerabilities of the system will be evaluated:*

A. *Is the encryption of the database implemented in a secure way and in such a way as to make meaningful manipulation of the database impossible?*

B. *Can the database be accessed outside of the GEMS or CTS system?*

C. *Are the program certificates of authentication implemented such that the certificates can be trusted to ensure application programs in use are the original unmodified federally certified applications?*

D. *Can the results from a ballot that was electronically duplicated be manipulated outside of the CTS application?*

E. *Is it possible to preview cumulated election results within or outside the system going around established procedures and if all security features (including smart card technology) are properly implemented?*

F. *Is the database replication among scanner units performed in a secure manner?*

G. *Is application level access control performed by the security module adequate – can rights, privileges, use of smart card, etc…be bypassed or escalated outside of the application?*

H. *Are the scanned ballot images stored securely? Is it possible to access ballot images by bypassing any security controls?*

1.3. Assessment Timeline

The following table summarizes the timeline for this assessment.

Date	Work Completed
2/3/2008	Vendor training of system, which was deemed too buggy to begin acceptance testing.
1/19/2009	Stable release accepted by KCE to begin acceptance testing. Security testing performed in concurrence with other acceptance testing activities.
2/11/2009	Mock Election #1 – failure.
2/16/2009	Mock Election #2 – failure.
2/23/2009	Mock Election #3 – failure.
2/26/2009	Mock Election #4 – failure. Software was determined was too instable to complete mock election. All testing was suspended while PES implemented bug fixes.
3/30/2009	Mock Election #5 – success. This was performed using the first bug fix release of the applications in response to the previous failures. Security testing was also performed during this week to review the new software versions.
4/20/2009	Volume Stress Testing, using the second bug fix software releases.
4/28/2009	Final testing by Anitian, to validate the bug fix releases, as well as other technical information provided by PES after the original deadline.

ANITIAN
ENTERPRISE SECURITY

2. EXECUTIVE SUMMARY

This section provides an executive level summary of Anitian's findings and recommendations.

2.1. Overall Assessment

It is Anitian's overall assessment that KCE can operate the new elections systems securely. This report details some risks that require corrective actions. However, as a whole the system is reasonably secure and KCE has done an effective job of developing good security procedures.

When evaluating the security of this system, Anitian evaluated the security of the KCE environment against the "three pillars of security" which are confidentiality, integrity and availability.

Confidentiality

Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. In the KCE environment, this meant the ability of PES systems and procedures to ensure confidential and sensitive data was not disclosed.

Anitian did not find any significant risks to the confidentiality of KCE systems or procedures. Any technical weaknesses that might allow for disclosure have been adequately remedied with effective procedures.

Integrity

In information security, integrity means that data cannot be modified without authorization. In an elections environment, this is a critical component. Anitian did extensive testing to ensure the integrity of election systems and data.

From a data perspective, Anitian did not find any significant risks to the integrity of election data. Effective procedures and policies are in place to compensate for any technical weaknesses.

Furthermore, the procedures, practices and safeguards in place would make it extremely difficult for an attacker to successfully alter the outcome of an election. While it is impossible to eliminate this risk entirely, it is Anitian's judgment that KCE has reduced this risk to an acceptable and reasonable level.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. For an elections system, availability is critically important during the time of an election. If systems were offline and unable to tabulate ballots, this could delay results and erode public confidence.

This is perhaps the only area where Anitian had concerns. There are some risks to the availability of elections systems, based on our analysis of the PES software and hardware. However, KCE and PES are working on these availability issues and Anitian saw tremendous progress in improvements to the stability of elections systems over the course of this project. When Anitian began this project, the election systems were very unstable and prone to crashing. However, at the conclusion of the project, the systems had become much more stable. And KCE had improved procedures to compensate for software instability.

There are still some risks regarding stability of the system. This report details these risks and recommends corrective actions KCE can take to remedy them.

2.2. Summary of Election Procedure Risks

It is Anitian's assessment that KCE's election procedures have areas of concern, but are generally sound overall. Some of the procedures were incomplete or undergoing modifications during this assessment, and were therefore difficult to fully analyze.

2.2.1.1. Ballot Cage Logs

The access logs to the ballot security cage are not readily available. The current system does not support detailed logging. In the event of a security incident, it would is very important to know exactly which people entered the cage and when.

2.2.1.2. Lack of Business Continuity Procedures

KCE currently does not have adequate business continuity (BC) procedures. This is partially understandable, since KCE recently moved into a new location and has new election systems. Nevertheless, KCE needs to make the development and testing of BC procedures a priority. It is important to not only develop the procedures, but also test them regularly to ensure they work.

2.2.1.3. Draft Procedure for Adjudication of Ballots

KCE has developed a draft procedure for electronic adjudication of ballots using the new voting system (Ballot Resolution – Electronic Adjudication (MB2-002 A). Anitian has provided suggested edits to the draft, however the overall design and content is sound.

It is extremely important for KCE to complete this procedure and publish a final version. Duplications, adjudication and determination of voter intent are complex processes that the public does not generally understand. Furthermore, it is an area of great concern for people worried about the possible manipulation of elections.

2.3. Summary of Elections Systems Risks

It is Anitian's overall assessment that the Assure system presents some risks to the availability of election systems. Anitian observed software that was unstable and prone to errors, particularly the earlier versions. Crashes and system errors resulted in an outright loss of data. This project required five separate mock election tests to achieve any level of success. Furthermore, the mock elections were not as complex as a full-scale election.

NOTE: *As this report was being finalized, KCE was performing volume testing using the updated versions of the software, during which there was a drastic improvement in the stability of the systems.*

Below is a summary of some of the most serious threats to the election systems, technologies and data, which are discussed in greater depth in section 4.

2.3.1. Deck Deletions

Anitian was able to scan a deck, and then, using the Central Count Server in GEMS, delete a scanned deck and remove all evidence of that deletion. Although this would require an insider to perform, it would be possible for a rogue user to essentially wipe out any deck and remove all evidence that they had done so.

While the potential impact of this threat is high, the overall risk is rather low. KCE already has strong procedures in place that mitigate this threat, such as their reconciliation procedure.

2.3.2. Accessible Vote Unit Card Tampering

Anitian was able to tamper with the memory cards that are placed into the AVU in such a way that the data from those cards could be corrupted without alerting the operator.

However, it would be very difficult for an attacker to successfully execute a card tampering attack. KCE has numerous procedures that provide very effective mitigation of this threat. Nevertheless, the threat does exist and warrants some attention.

It should be noted that Anitian was not able to change votes. Rather, our testing was able to modify aspects of the memory card such that votes could be unintentionally cast or ballots being uncounted due to configuration corruption.

3. PROJECT PREMISES

Complex risk and security testing requires a solid understanding of the environment and influencing factors that comprise the entire test. This section defines some of the premises, assumptions and given facts that Anitian used throughout this project.

3.1. Philosophical Approach

A security and risk assessment is ultimately the product of a group of people. How people work and the approach they take can have a significant impact on the overall results. This section describes how Anitian philosophically approached this project. It is important to understand our approach, since it forms the framework for our analysis, and ultimately, our results.

3.1.1. Understanding Risk

In the realm of information security, the word risk has a very specific meaning. The risk of an individual threat happening is the product of the probability and impact (also called exposure) of that threat. Therefore, to evaluate the risk of any threat, we must analyze both the impact of that threat and the probability of the threat source successfully exercising the vulnerability.

Risk, probability and impact can be expressed as a mathematical equation:

```
Risk = probability x impact
```

For example, if we rank probability on a scale of 0 to 5, with 0 being impossible and 5 being almost certain, and impact having the same scale of 0 being no impact and 5 being catastrophic impact, then risk would have a scale of 0-25, with 0 being no risk at all and 25 being a very serious risk. Notice, that anytime either one of the factors is 0, the risk is also 0. This is important. A threat may have a very large impact, if it occurred, but the probability could be 0, or impossible. Thus, the threat as a whole has no risk.

Realistically, there are many threats that have almost no probability of happening in the normal functions of an elections environment, although we can rarely assume them to be impossible. Moreover, some threats are actually *compound threats*. That is, multiple threats must occur in a specific sequence or within a certain reference to result in a final threat.

One common mistake in risk analysis is to create threats that require highly improbable sequence of events. The most common example of this is the *cascading failure with no response* threat. While it is not impossible for multiple systems to fail or be compromised at the same time, it is very unlikely that if this happened, operators and support staff would not respond and allow it to continue. When systems begin behaving incorrectly, people will naturally take steps to correct the problem, particularly in a closed environment such as at KCE. As such, any threat that depends on a complex sequence of events over an extended period of time, without any response from election staff, would be considered an improbable threat, unless there were particular factors in the threat that prevented staff from being aware of the event.

For Anitian's risk analysis, we focused on those threats that presented the most significant probability of occurring. As the next section explains, probability also has a very specific meaning in the realm of risk analysis.

3.1.2. Understanding Probability

One of the most relevant aspects of this assessment is the probability of a threat actually happening. All security threats can be classified in one of three ways: impossible, possible, and probable.

An impossible threat is something that could not reasonably happen. A possible threat is any threat that could possibly occur with no consideration of the likelihood of that threat actually happening. A probable threat is a threat that is not only possible, but has a reasonable likelihood (or probability) of actually happening.

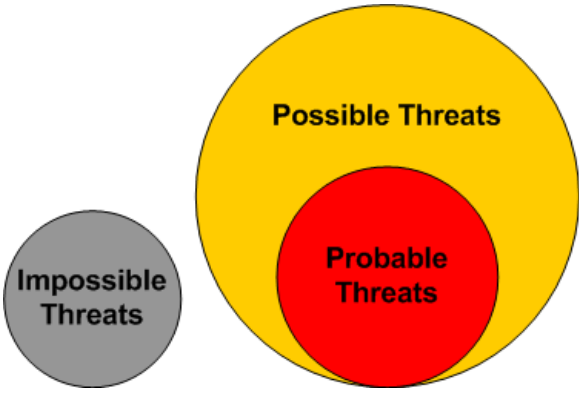

Figure 1 – Diagram of the relationship between threat types.

For example, the possibility of a group of rogue political operatives bribing KCE staff to install a specially targeted virus that causes a catastrophic, cascading failure of all election systems with no incident response from election staff is a possible threat, but not probable. The failure of a few counting systems due to software misconfigurations or failure is a probable threat.

The number of possible threats is very large, numbering thousands or millions. Those threats can include a wide array of obvious, obscure and exotic threats. Some of which can be quite sensational and terrifying. However, many of those types of threats are not specific to the system(s) under consideration. These general threats are more applicable for a general risk assessment or business continuity analysis.

Since there is a limited amount of time and resources to any security analysis effort, Anitian focused our time and efforts on those threats that have the highest probability of occurring. Exotic and sensational threats are only evaluated if they have a reasonable chance of occurring and have a reasonable chance of causing a failure of some type.

3.1.3. Practical, Operational Approach

The other critical aspect of this project is KCE's decision to focus exclusively on the practical, operational aspects of the Assure voting system. Anitian did not perform a review of the software code. Anitian focused on the operation of the Assure voting system, and how KCE staff and the public interacted with the components of this system. Anitian also evaluated the overall security of the systems and environment hosting the Assure applications.

Software and hardware does not operate in a vacuum. It must be installed, configured, managed, monitored and used. People and other systems must interact with that software. It is Anitian's experience that how an application is installed, configured and used has a more profound impact on the security of the overall system than the actual software itself.

An inherently insecure application can be deployed and used in a secure manner if there are sufficient controls to mitigate the application's weaknesses.

For example, storing confidential data in an unencrypted file is undesirable and insecure. However, if mitigating controls are implemented that monitor the data, restrict access to it and control its dissemination, then the risk of threats that depend on the data being unencrypted decrease. It is possible to create an environment that provides the secure operation of an insecure application through effective mitigating controls.

However, the reverse of this is just as true. A well designed and fundamentally secure application can be deployed, used and configured in a very insecure manner.

3.1.4. Scientific Methods of Analysis

Anitian embraces the core tenants of the Scientific Method to conduct our security and risk assessments. This methodology is the fundamental basis for all scientific research and analysis. It also is specifically intended to eliminate personal bias and opinion and focus on observable facts.

The following diagram highlights the basic components of Anitian's methodology.

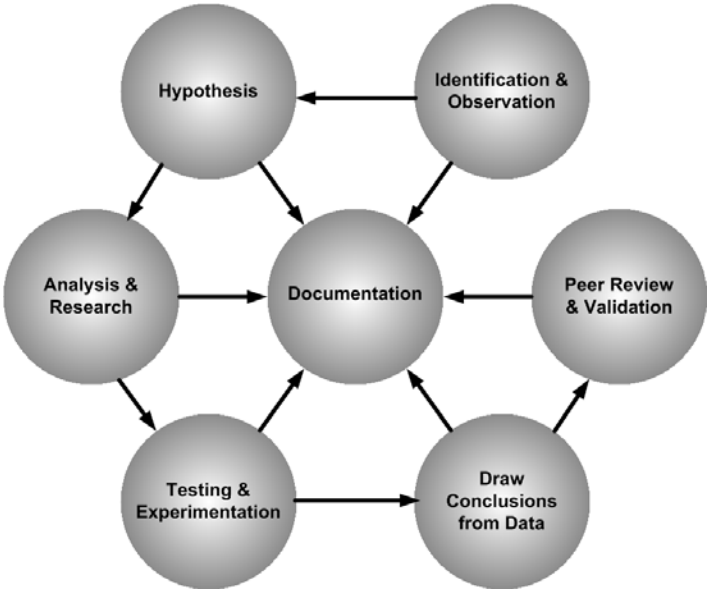

Figure 2 – Anitian's Exclusive Scientific Assessment Methodology.

Our methodology consists of these components.

- **Observation**: Anitian observed the operation of the elections system and read all background documentation and reports.
- **Hypothesis**: Anitian theorized on the most likely ways the system would be compromised based on an objective analysis of the system components, procedures and data. The intention of this phase is to rule out risks and methods that are theoretically possible but highly unlikely.
- **Analysis & Research**: Using our observations and hypotheses as a guide, Anitian analyzed and researched the issues, technologies, configurations and designs of KCE's environment.
- **Testing & Experimentation**: Based on our research and observations, Anitian conducts appropriate tests to prove our hypothesis and deliver empirical evidence.
- **Draw Conclusions**: After testing and analyzing the KCE's environment, Anitian draws conclusions and crafts recommendations based on the data we have gathered.
- **Documentation**: Along the way, Anitian has documented everything. This includes writing a comprehensive, yet readable report.
- **Peer Review & Validation**: The last step is to subject all our findings, evidence and analysis to peer review. This step is critical in ensuring our work is of the highest quality.

3.2. Definitions

This section outlines some terms and common usage for this report.

Term	Definition
ASM	Assure Security Manager. The application that creates and manages users, roles, database and application privileges.
ASS	Assure Security Service. Provides authentication and authorization for the Assure environment.
Assure	Assure 1.2 voting system developed by Premier Election Systems. This is the umbrella term used for all of the system components provided by Premier under review.
AVC	Accessible Voting Center. A location where AVUs are available for the public to use.
AVU	Accessible Voting Unit. Touch-screen voting system, intended for special needs voters.
DTNP	Distributed Tally Network Protocol. Used by Premier's Central Scan application for the purpose of data transfer and synchronization between collaborative workstations on a tally network.
GEMS	Global Election Management System. The primary tabulation and control application.
KCE	King County Elections.
KCT	Key Card Tool. Software used to create public/private key pair used for elections.
PCS	Premier Central Scan. The tabulation software that runs the scanning hardware.
PES	Premier Election Solutions, formerly Diebold.
PS900	DRS Photoscribe PS900 iM2. An image-based scanner used with PES' PCS to scan and count AccuVote-OS paper ballots.

Term	Definition
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. Throughout this document, the following terms will be used to qualify risk.
	None — The threat poses absolutely no risk to an election process or the integrity of the tabulation. Low — The threat poses a low risk to election integrity or security. Corrective actions are advisable, but not critical. Moderate — The threat poses a moderate risk and demands corrective actions. High — The threat poses a high risk and corrective actions should be implemented immediately.
Scanning Room	The location in the KCE facility where ballots are run through the scanners.
Severity	The magnitude of impact of a threat successfully exploiting a vulnerability. All threats have a severity, based on the impact that threat would create if it were to happen.
Threat	Any circumstance or event that has the potential to cause harm, specifically to either the confidentiality, integrity or availability of the system and/or the data.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability, or a situation and method that may accidentally trigger a vulnerability. Sometimes referred to as a threat agent.
TN	Tally Network.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

3.3. Test Environment

Two separate environments were used for testing, both of which were deployed and maintained by PES. The first was the production environment that KCE was using for Acceptance Testing, of which this Security Review was a component. This environment underwent multiple architectural changes, but ultimately consisted of the following components:

- 1 x Cisco C3560G-48-TS-S Switch.
- 1 x GEMS Server.
- 1 x ASM Server.
- 1 x Windows Domain Controller.
- 1 x PCS management workstation – Adjudication workstation that downloads the workspace from GEMS and seeds the TN.
- 2 x DTNP Hubs - Adjudication workstations that do not have an open workspace.
- 7 x Adjudication Workstations.
- 11 x PS900 Scanners.
- 8 x AVU – Seven are used for casting votes; one is for uploading results to GEMS.

Anitian spent an extensive amount of time observing the various phases of acceptance testing using the production hardware at KCE. The second environment was a test lab that was created specifically for this Security Review. It consisted of the following components:

- 1 x Cisco C3560G-48-TS-S Switch.
- 1 x GEMS Server.
- 1 x ASM Server.
- 1 x Windows Domain Controller.
- 2 x PS900 Scanners.
- 1 x AVU.

3.4. Software Versions

Over the course of the security review, there were changes to the source code to addresses numerous software errors uncovered during acceptance testing. After four failed mock elections, PES issued new software code, which is referred to as the "first bug fix" release. Since Anitian had performed our testing on older versions of Assure, follow-up validation tests were performed.

Immediately after Anitian completed our follow-up tests, PES released a "second bug fix" release for use in the volume testing. Anitian returned and conducted a review of these fixes. KCE was uncertain if another Mock Election was needed to validate these new fixes. Anitian advised KCE that a second Mock Election seemed unnecessary, since any significant bugs would be uncovered in the volume testing.

Anitian asked PES for a list of all the software changes that were made, so another round of validation tests could be performed. PES initially denied this request, citing resource constraints on the development team.

Anitian was scheduled to release this report on April 24, 2009. On April 23, 2009 PES provided Anitian with a report that listed the fixes and changes made in the two bug fixes. The report was a simple copy and paste from the bug tracking software used by the Assure developers. Anitian is familiar with the general class of bug tracking software used, and the information would have been available as soon as the bug tracking entries were originally created. PES did not provide any explanation as to why this information was not provided earlier, or more importantly, why it was delivered literally hours before Anitian was scheduled to deliver this report.

This bug fix information included changes to areas of the applications that neither Anitian nor KCE were aware of. It was apparent that PES had changed the software from the time of the fifth and final mock election and the volume testing. However, the final version numbers citied in the bug tracker did not match those deployed at KCE for the volume testing.

When asked to explain these changes, Anitian received the following response from PES:

> *All of our four digit versions like the ones you tested are rolled up and referred to as three digit builds when submitting or dealing with certification authorities. So the version you looked at GEMS 1.21.1.1 is the exact same as the referenced rolled up version 1.21.2 and so on for the other products in the suite. Since the three digit rollup for the mock had changes to it, it's first iteration of change would be the four digit 1.21.2.1 and so on, thus then rolling up into 1.21.3.*

This is not a standard software development practice. Standard practice is to release beta versions or "release candidates" for testing, and then provide stable release versions to customers for production. Also, two releases with different version numbers are always assumed to be different in some way. Based on PES's explanation, they are releasing software with different version numbers, but stating they have the same code.

As a result, Anitian cannot verify that the versions that Anitian tested are exactly the same as those submitted to the EAC. Consequently, this report might not be applicable to the versions PES submitted to the EAC. PES asserts that the versions Anitian tested and the versions submitted to the EAC are the same. However, Anitian cannot validate this claim.

KCE expressed some concern with Anitian that the last version was not run through a mock election. However, based on Anitian's understanding of the volume testing and other functional testing KCE has planned, another Mock Election does not seem necessary. .

The table below shows the different version numbers tested by Anitian, and submitted to the EAC as this report was being completed.

Application	Original Version Tested	First Bugfix Version Tested	Final Version Anitian Tested	EAC Submitted Version
GEMS	1.21.1.1	1.21.2.0	1.21.2.3	1.21.3
ASM	1.2.0.21	1.2.1.4	1.2.1.5	1.2.2
PCS	2.2.0.31	2.2.1.4	2.2.1.5	2.2.2
AVU	Firmware - 4.7.3.2 (pre-release) OS - WCER7-410.3.10 Boot loader – BL-1.3.10 AVPM firmware - Model 3 Rev 0 (3.0.3)	No change	No change	4.7.4
KCT	4.7.2.1	4.7.3	No change	4.7.4

3.5. Limitations and Considerations

There were some limitations to this Security Review. This section outlines some of these general limitations and considerations.

3.5.1. Code Review Limitation

A formal review of the Assure voting systems code was not in-scope for this project. It was determined during the course of the project that some requests in the Work Order could not be performed without a comprehensive code review. For those instances, the concern or issue was presented to PES requesting a statement on how the issue had been resolved and/or remediated. These requests were reiterated in conjunction with KCE personnel several times in an attempt for them to be fulfilled.

Primarily, these were the four flaws identified in the report "Software Review and Security Analysis of the Diebold Voting Machine Software" commissioned by the Florida Department of State, released in December 2007.

PES did not respond to these requests until the afternoon of Thursday, April 23rd, 2009, one day before this report was originally due. PES explained that their extremely limited development staff were focused on bug fixes and did not have time to respond.

Due to an extension of the delivery date by KCE, Anitian did ultimately have time to review and validate the claims made by PES in regards to the items cited in the report, for those that did not require a code review.

3.5.2. PES Response Delays

Anitian requested specific information on the bug fixes that were implemented during the final weeks of this review. Information about these bug fixes was not supplied to Anitian, via KCE, until the evening of April 23rd, 2009, one day before Anitian was originally scheduled to release this report to KCE.

As a result, KCE extended the delivery date for this report so that Anitian could validate the bug fixes and other technical information PES provided. Anitian also reviewed the second bug fix version that PES deployed for volume testing.

Anitian also requested documentation on the technical specifications on the DTNP protocol at the beginning of this project. Once again, PES stated that they did not have resources to complete this document.

Since documentation was unavailable, Anitian conducted an independent analysis of the protocol, which is discussed later in this report. Just prior to the final delivery date of this report, PES finally provided Anitian with the DTNP Protocol Specification.

Based on these observations, Anitian recommends that KCE establish very clear deliverable requirements and deadlines with PES. During the course of this project, PES demonstrated an inconsistent ability to deliver documentation and resources to KCE. This represents a risk to KCE.

3.5.3. On-Going Software Development & Insufficient Testing

The applications and operating procedures underwent extensive changes throughout the test period. All of the documentation PES provided was in draft form, and they contained numerous inconsistencies.

Anitian observed PES improvise new procedures as acceptance testing repeatedly failed. At times it appeared that Assure was undergoing a collaborative QA testing rather than a controlled implementation of an established application. Furthermore, when procedural changes were made, regression testing was not performed.

During the course of this assessment, there were a total of five mock elections conducted. The first four were complete failures. With each failure, acceptance testing was placed on hold while the Assure development team would identify the errors and attempt to fix them. Most of these changes were procedural, although ultimately new code was rushed into production. Many of the problems appeared indicative of insufficient scalability. According to PES representatives, the KCE environment was by far the largest deployment of the application, resulting in several different proposed architectures until the environment could be stabilized. Examples of the changes included the introduction of two dedicated PCS workstations that served as DTNP hubs, active on the TN, but without an open workspace. There were also changes to how the election was downloaded from GEMS and seeded on the TN.

Anitian advised KCE several times that the two to three week timeline allotted for the emergency bug fixes was insufficient to perform thorough regression testing. This was particularly important since PES could not identify the exact reason for the errors. The numerous changes to the operational procedures exacerbated this problem, making it difficult to determine if the errors were procedural or software bugs.

Furthermore, PES repeatedly deployed versions of the Assure applications to production that continued to fail, resulting in emergency bug fixes.

3.5.4. Architectural Changes

Throughout the testing, the architecture changed numerous times in response to errors uncovered during testing. Eventually, the test lab and the production environment were not the same. However, the PES staff did attempt to create a similar environment in spite of what ultimately became hardware limitations, due to the introduction of new system roles in the TN. For example, PES implemented the use of a dedicated TN hub, which was simply a PCS workstation on the TN without a copy of the workspace. This was not implemented in the test lab. However, one of the other new roles on the TN was to have one of the scanners servers serve as a workspace management workstation. This was adopted in the lab, leaving only one PCS workstation to perform the scanning. Also, originally, a copy of PCS was running on the ASM to serve as the adjudication workstation in the test lab. After the first bug fix release, the ASM was rebuilt as a standalone host, and adjudication was performed on the workspace management workstation.

3.5.5. Systems No Longer in Use

The original Work Order referenced a system that is no longer in use at KCE, the AccuVote-OS.

4. OPERATIONAL PROCESSES AND PROCEDURES

This section of the report outlines the threats and risks associated with the processes and procedures in use at KCE to generate election materials, conduct an election and tally votes.

While this report is primarily a security review for the new vote tally system being installed by KCE, ballot security does not begin with the tally of votes. Ballot security begins early in the process; at the point the contests for the ballot are created.

KCE uses a mail-in election environment with an allotment of touch screen systems for people with special needs. The production of an election has the following general phases:

- Ballot creation.
- Printing.
- Ballot distribution.
- Ballot return.
- Processing (open, inspect, duplicate, etc...).
- Tabulation.
- Archiving.

Anitian reviewed the entire life cycle of an election, from the creation of an actual ballot in both electronic and paper form through to the final archiving of counted ballots. Anitian evaluated both written procedures and observed elections staff carry out the normal duties of producing an election. The elements of this review included:

- Review of the King County Security Plan.
- Review of written procedures as provided.
- Evaluation of the elections facility.
- Observation of operational procedures in the February 3, 2009 election.
- Observation of the mock elections (there were five total attempts, four failures and one success).
- Election setup.
- Review of ballot scanning procedures.
- Review of ballot adjudicating procedures.

Some of the processes KCE uses were in a state of flux when Anitian observed the mock elections. Some processes had not been developed at all and others required more extensive testing. While many aspects of the procedures are properly designed and executed, Anitian's mandate was to identify those areas of concern. The following sections define the relevant threats and their associated risks for a variety of issues.

4.1. Security Plan Review

The section below contains findings from our review of the King County Elections Security Plan, dated January 21, 2009 (Quoted and italicized text is taken directly from the security plan document).

4.1.1. Ballot Security Cage Physical Access Control Logs

Risk: High

Blank Ballot Stock Security (p. 8) - *"All live voted mail and provisional ballots and all printed ballot stock are secured in a cage when not actively being processed. Per the Access Control section above, these cages are secured with biometric key card access, which limits access and records ingress/egress on an access log. Only authorized personnel have access to these areas, and uniquely numbered seals are used to provide accountability of access."*

Recommendations

Anitian understands that there is some delay in producing these logs because of a lack of funding to enhance the reporting capabilities. Nevertheless, reporting capabilities should be enhanced to provide timely access logs. These logs should be made more easily available to election observers for review. Data is available for specific instances of concern, e.g. review a door that may or may not have been opened. However, the records are not readily available, and would require an incident requiring investigation or a public disclosure request on behalf of the public.

4.1.2. Storage of Video Surveillance Tapes

Risk: Moderate

Video Surveillance (p.6) - "*All video is recorded 24/7 to a DVR that will be retained for the same period of time required for other elections material. For federal election, this is 22 months and for all other elections 60 days."*

Storing surveillance tapes on-site is an unnecessary risk. They can be destroyed due to a disaster at the facility, or even stolen by a thief.

Recommendations

Store recorded tapes in a secure, off-site location.

4.1.3. Access Control Deprovisioning Procedures

Risk: Low

Key Control (p. 6) - *"Keys and county identification are collected upon termination. Should a keyed door be compromised through the loss of a key, Elections staff will take immediate action to have the appropriate door(s) re-keyed.*

KCE is already using a form to deprovision accounts and performs regular audits of accounts. This is a good practice. However, there could be more formality to the process.

There is already a form that management uses to deprovision accounts when someone leaves. It would be preferable to have a form for each user that tracks rights as they are granted. When that user leaves, that form can be used to ensure all access is correctly rescinded.

Furthermore, KCE performs regular audits on all computer accounts and access controls to ensure that they are issued to active employees.

Recommendations

KCE's practices in this area are good and in many ways meet best practices. However the process of deprovisioning accounts needs to be more formalized.

First, KCE should change the provisioning process to use a form for each employee, listing which rights are assigned to them. This should then be integrated with a formal, documented deprovisioning process that is triggered upon separation.

Furthermore, the entire rights management process should be documented in greater detail, including the procedures and schedule of regular audits.

4.1.4. Insufficient Security Training

Risk: Moderate

Personnel (p.7) - "Training about areas of responsibility, sensitivity of information, security of ballots, and chain of custody for the ballots is necessary for all employees and volunteers, and is accomplished through individual work units in training and orientation by work group leads and supervisors."

When Anitian asked about security training, we were provided information that was applicable only to temporary workers. Security training for only temporary workers is insufficient and does not correlate to the written policy. KCE clarified that all staff receive computer security awareness training. Furthermore, all permanent staff in the ballot processing area attend the same training as temporary employees.

Recommendations

It is important that staff not only receive training in computer security, but also specific training in elections security. The current training and awareness being performed does not specifically address the issues surrounding elections security.

Develop a policy that requires all staff to undergo regular security training, which specifically addresses matters of elections security. Documentation should be available that demonstrates that training was conducted and staff has attended.

4.1.5. Insufficient Review of Ballot Print Logs

Risk: Moderate

Blank Ballot Stock Security (p. 8) - "In the Elections office mail ballots are issued to voters over the counter using the Ballot-On-Request (BOR) module. Blank ballot stock used to print these in-house ballots is tracked by a stub numbering system and an audit log. This stock remains in secure storage when not in use. Only authorized elections staff have access to the blank ballot stock and the ability to issue ballots using the BOR module. This function is assigned only to full time elections staff. These individuals are specially trained to issue and produce ballots using the Ballot-On-Request (BOR) module. At close of business each day, the BOR operators log out of the system. The Superintendent of Elections or a designee is responsible for reviewing the audit logs and coordinating ballot accountability."

KCE staff told Anitian that the reviews of the audit logs "are conducted as needed."

Recommendations

KCE should have an established schedule to review the audit logs. The results of each review should be documented.

4.1.6. No Criminal Background Check on Temporary Employees

Risk: Low

Personnel (p.7) - "A dedicated elections staff recruiter focuses on hiring qualified temporary employees to assist with the various tasks of administering an election."

Recommendations

While it would be very desirable for KCE to conduct complete criminal background checks on all temporary staff, the cost and complexity of doing so may not justify the results. Anitian is unaware of any reliable statistics on how many criminals work as temporary elections staff, and the threat that may present, making this risk difficult to quantify.

KCE should implement criminal background checks for all temporary employees at some point. However, there are other issues that are more serious and address more immediate concerns. As such, this issue was downgraded to low risk.

4.1.7. AVU Proofing Policy Inaccurate.

Risk: Low

Accessible Voting Units (p.9-10) - *"Before opening each AVC, a "zero proof" printout from each voting machine verifies to AVC workers there are no votes stored on the memory card and that the races are properly coded for the election."*

Recommendations

The Accessible Voting Center (AVC) workers review the "zero proof" printout to verify that no votes are stored in the memory. However validation that the races have been properly coded for the election is performed prior to this step, and is not a part of the zero proof examination. The security policy should be revised to reflect actual process.

4.2. Operational Procedures Review

Anitian reviewed all of the procedures that KCE provided. This section focuses on the operational procedures. Technical procedures are reviewed later in this document. In reviewing the operational procedures, there are three basic results.

4.2.1. No Security Concerns

The following operational processes were observed in the live election which was conducted on February 3, 2009. Anitian did not identify any threats with a significant risk in these processes.

- Procedures for Using Pitney-Bowes Sorters MB2-020 C.
- Mail Ballot Privacy Flap Removal MB2-005 C.
- Verification Procedure MB2 014 G.
- Reconciliation MB2-010 F.
- Opening MB2-003 C.

Anitian did not identify any significant risks with the following procedures:

- Processing Mail from 24 Hour Drop Boxes MB2-021 B.
- Ballot Pick-up Staff Procedures at Libraries.
- Batch Uploads MB2-22 H, MB2-006 D, MB2-008 C, and MB2-007 C.
- Final Elections Reporting TS2-014 A.
- Manual Insertion Procedure MB2-012 G.

4.2.2. Procedures Needing Revision

If the new vote tabulation system is implemented, then the following procedures need to be revised to reflect the processes.

- Tabulation of Ballots MB2-015 F
- Duplication MB2-001 A-4 (Need new procedures on electronic adjudication)
- Election Tabulation TS2-010 B (Initial elements in GEMS preparation may be valid, but need to be reviewed)
- GEMS and Tabulation Testing TS2-006 A (Some testing processes will generally follow existing procedures, but will need reviewed and revised based on new system.).
- AVU Memory Cards – Handling and Recovering Failed Cards During an Election TS2-001 B (Needs updated to reflect elimination of polling places and existence of AVC.)

4.2.3. Procedures with Security Concerns

The following risks were identified with the procedures.

4.2.3.1. Insecure Ballot Data Exchange

Risk: Low

Ballot Building TS2-015 -

Page 3: ***1.0 Create a Ballot Export file from DIMS*** – *"12) Outside of DIMS, copy the file to a CD for transport to the GEMS Ballot Building Server."*

Page 4: ***3.0 Import DIMS Ballot Export file into GEMS*** – *"1) Load the CD containing the DIMS file that was saved in step 1.0."*

Anitian observed KCE staff using a flash drive to transport this data, although the policy calls for a CD. Furthermore, this transport was unsupervised.

KCE's ballot proofing and L&A processes mitigate any possible tampering with ballot data. It is unlikely that malicious code would be introduced without detection. Each night scripts are run on the GEMS system that would detect any changes to files. The Secretary of State provides these scripts and Anitian verified that they are being used correctly.

Recommendations

KCE should ensure that the procedure is being followed as documented, or update the procedure to reflect their practices.

4.2.3.2. Lack of Observation and Supervision of Ballot Creation

Risk: Low

Ballot Building TS2-015. The policy provides for "last minute change" but provides no oversight or documentation requirements. While procedural practices would make it nearly impossible for an unapproved change to be introduced, any such changes should be documented.

Recommendations

It would be preferable to have a second person observing all functions in ballot creation and any changes needed. However, Anitian understands this may be "economically onerous" to KCE. However, at a minimum KCE should require documentation of any changes made after the ballot was created. Also, this procedure needs to have references to "polling places" removed.

4.2.4. Lack of Security Agreements with Printing & Inserting Vendor

Risk: Moderate

Machine Insertion Procedure MB2-013 C. As written, this procedure is sound. However, there is a concern that there is no agreement that defines security practices as it relates to off-site vendor. Currently there is one vendor who prints the ballots, inserts and delivers them to the U.S. Postal Service for mailing.

The only security information that exists regarding the custody of the ballots during the time when the vendor has custody of the ballots is a generic "Security Overview" provided by PES which generally references key pads, digital cameras, and so forth.

Recommendations

The Elections Division should require a very specific security agreement with any vendor(s) who have custody of ballots outside the election facilities, regarding the custody and security of ballots.

This agreement should cover the following:

- Explicit requirement for the vendor to keep ballots secure at all times and control access to only those people who require access to complete their job.
- Transportation security.
- Chain of custody.
- Audit logs for access to areas where ballots are stored.
- Accounting logs that show what quantities of ballots were printed, processed, damaged, and unused.
- Details on vendor employee screening and background check procedures.
- Such security agreements should be renewed, or at least reviewed, annually, and monitored for compliance.

4.2.4.1. AVC Memory Compartment Handling

Risk: Moderate

The procedure for daily closing of the AVC specifies that the seal over the memory compartment is to be inspected to ensure there has been no tampering. Nothing in the closing procedures addresses how the memory cards are to be handled when the AVC voting is concluded.

If they are removed, there are no instructions as to what is to be done with them. If they are not to be removed, there are no instructions as to how the AVUs are transported and what the process is for getting the memory cards from the units.

Recommendations

Amend procedure to explicitly define how all aspects of closing will occur at the end of AVC voting. This should include:

- How memory cards are handled.
- How they are secured.
- How memory cards are transported to the operations center.
- How memory cards are stored.
- Detailed chain of custody logging for all memory cards as they pass from one person to another.

4.2.4.2. Handling of Memory Cards from Provisional Ballot AVU

Risk: Moderate

Accessible Voting Center Provisional Ballot Procedures (unnumbered). At least one AVU is designated for the casting of Provisional Ballots. The paper tape from these units is disengaged so the paper record of the voting can be placed into the appropriate provisional ballot envelope as law requires. The memory card in the provisional ballot AVU should not be uploaded for counting as are the memory cards of the other AVUs in the Accessible Voting Center.

Recommendations

KCE needs to develop specific procedures to ensure the memory card from the provisional ballot AVU is not included with the other memory cards or AVUs. The procedure should include explicit handling instructions for workers. The cards should be clearly labeled as provisional to ensure they are not confused with other cards.

4.3. Disaster Planning and Recovery

Given that there have been a large number of changes and activities within KCE in the recent past (new systems, new processes, new facility and a presidential election, to name a few), it is understandable that KCE has not developed a complete Disaster Recovery Plan (DRP). Nevertheless, this is an area of concern that demands immediate attention.

Election offices are certainly prone to emergencies. Election offices nationwide have experienced all types of emergencies including bomb threats, explosions, vandalism, earthquakes, roof cave ins, fires, power outages, virus and chemical attacks, and even vehicles crashing into buildings.

Effective DRPs can not only save lives, which is the primary purpose for such planning, but in some cases can protect valuable information and ensure the integrity of the elections process.

4.3.1. Authority for Building Emergencies

Risk: High

No written procedures exist for command and control in the event of building emergencies. Clear lines of authority should be delineated between facilities management, elections management and county security.

Recommendations

A clear command and control operational structure must be developed among the various county agencies with responsibility for the elections facility.

4.3.2. Emergency Management Responsibilities

Risk: High

There is no documented emergency management structure specifying responsibilities for the various election systems under emergency circumstances.

Recommendations

The Elections Division must develop written policies identifying responsibilities for various election systems in the event of an emergency. These policies should provide for alternate assignments for various systems if the primary assigned person is not available.

4.3.3. Insufficient Uninterruptable Power Systems

Risk: High

Uninterruptable power systems (UPS) are in place for the GEMS servers, security servers and network switches. However, due to a change made during construction, the tabulation room is not currently equipped with UPS backup. Staff commented that they are currently "scoping the best options" for adding this capability.

Recommendations

High priority must be given to providing effective emergency backup power to the tabulation room, at least to the extent to allow a controlled shutdown of the tabulation system without loss of data.

4.3.4. On Site Storage of System Backups

Risk: Moderate

The GEMS data is backed up regularly and stored in a different location in the building. While this is procedurally sound, it is preferable that the backups be stored at a secured offsite facility.

Recommendations

The backups of GEMS data should be kept in a secure storage facility at a different site than the Elections Office. Anitian recommends KCE establish a secure storage facility elsewhere in King County or the metropolitan area. Given the sensitive nature of ballots and election systems data, Anitian suggests that KCE not use a third party storage facility. Rather, KCE should consider using another secure KCE facility, in order to retain complete control of the facility's security, including personnel.

4.4. KCE Facility

Election managers nationwide would likely envy the King County Elections offices. The offices have ample space, opportunity for process separation, adequate security and sufficient parking. It is rare to find a facility with all of these elements.

From a security perspective, the facility is better than most. Some of the major security features include:

- "Caged" spaces for secure processes which provide not only security but transparency.
- Card access entry system.
- Biometric entry system into high security areas.
- Open ceilings.
- Color coded wiring.
- Video surveillance in secure areas.
- Secure areas (Server Room and Ballot Tabulation Room) cabled securely.
- Certain doors are alarmed.
- Visitors must check in.
- Procedures are in place to control access to the facility's computer network(s).

4.4.1. Visitor Check-in Process Deficiencies

Risk: Moderate

KCE requires visitors to be checked in and issued a visitor badge, which is good. However, Anitian observed that the area for checking out visitors at the end of the day closes before the end of the business day, when visitor may still be present.

The threat here is that a person, who is intent on causing trouble, could hide in the building until everybody has left for the day. This person might not be discovered until they have compromised key systems or caused serious damage.

KCE has implemented effective mitigating controls to detect the presence of an unauthorized person. However, any response would be delayed. During that delay, a motivated person could cause significant damages to election systems and facilities.

Recommendations

The visitor check-in/check-out process should be evaluated to determine if it is meeting the expectations of management. While the risk is moderate, the potential impact is high. Therefore, Anitian recommendations that KCE revise their processes to include an end of the day sweep of the building or confirmation that all visitors have been checked out.

4.4.2. Color Coded Network Cables Are Visible In Public Areas

Risk: Moderate

KCE is using a color coding scheme for their network cables: white for access card biometric entry, yellow for security cameras, red for fire alarm system, blue for the business network and gray for the tabulation system. This is a good practice, in general.

However, all of the cables, except the gray tabulation cables, are exposed throughout public areas on the second floor.

It is feasible that a person could cut the cables to disrupt system availability or install a network tap to intercept communications thus compromising confidentiality and integrity.

Anitian understands that the intent of having these wires visible is to provide transparency to the public. There are ways to provide the same level of transparency while still physically securing the cables. For example, the cables could be secured inside clear plastic tubes.

Recommendations

These wires should be physically secured. Anitian suggests KCE review the location of these cables and determine if clear plastic tubing or other barriers can be implemented to provide physical security.

KCE should conduct disconnection tests on these cables to see how they respond to failure, in order to evaluate the consequence of this threat.

4.4.3. Weaknesses in Physical Access Controls

Risk: Low

The biometric and card access controls have some serious operational deficiencies. Anitian observed the following:

- On numerous occasions, personnel were "piggybacking" into a secured space. Piggybacking is when one person is authorized entry, then holds the door open (either purposefully or inadvertently) and another person(s) enter the space without authorizing their access.
- Certain spaces require cards to enter, but not exit, which means the duration of access cannot be tracked. High security areas can be exited without a card, but an alarm is sounded.
- False alarms were common. Anitian did not observe any local response to alarms. It is Anitian's understanding that the security office in Seattle phones KCE each time an alarm is sounded, describing the activity seen on the security cameras, for KCE to validate.

Recommendations

Anitian recommends the following:

- Entry and departure protocols for secure spaces should be firmly established and enforced. Employees should be trained not to "piggyback" with other authorized staff or allow other staff to do so to them.
- A clear understanding of what is expected of the secure entry system should be developed. Questions relating to the level of tracking expected (entry, exit, occupancy) need to be answered and the system (or expectations) should be adjusted.
- Policies should be developed that require users to respond to any and all alarms, particularly during an election cycle.

4.4.4. Fire Suppression System Concerns

Risk: Low

The fire suppression system uses water, exclusively. They are a wet pipe, also called closed head system. Being fully "charged" with water, whenever a fire is detected, the entire system discharges immediately. This generally occurs when the temperature on the sprinkler head nozzle exceeds 165 F, melting the nozzle and allowing the water to flow. While this is a relatively standard situation in election offices, it should be noted as a risk since a small fire elsewhere in the building might trigger the fire suppression systems in an area where paper ballots are stored or in the tabulation or server areas, causing a significant disruption to election processes and the security of the ballots and/or tabulation systems. Furthermore, these systems are susceptible to nozzle failure, and pipes can freeze and burst if exposed to cold weather.

Recommendations

King County should consider covering all paper ballot storage with plastic to mitigate damage due to sprinkler discharge or pipe failures. Disaster recovery procedures for the Assure systems should consider recovery from these events as well.

4.5. Review of Election Processes Observed During February 3, 2009 Election

Anitian reviewed all processes from the time the ballot envelopes arrived at the King County Election Center until they were being tallied (on the current optical scan system).

Anitian reports the following general observations.

- All processes are very detailed.
- Each functional supervisor has a manageable span of control.
- Security and accountability are integrated into all processes and enforced by supervisors and staff throughout.
- A generally secure facility and workflow are assets to the process.

The following processes were observed:

- Flap Removal.
- Sorting and Signature Capture on Pitney-Bowes equipment.
- Signature Verification.
- Reconciliation.
- Secrecy Envelope and Ballot Removal.
- Duplication.
- Tabulation.

4.5.1. AVCs

As part of the Election processes, Anitian observed the opening and closing of the AVC at the KCE Center. Anitian also then visited a remote AVC in the Bellevue City Hall.

The daily opening and closing procedures exactly matched the well written procedures. A sufficient number of staff was available and the checks and double checks were meticulously followed. Overall, staff performance and professionalism were quite high.

4.6. Mock Elections Review

In total, there were five separate Mock Elections. The first four Mock Elections failed. On each occasion, PES revised processes and software configuration (and in one case code) in response to the failures. The fifth mock election was able to complete successfully.

While Anitian was on-site for observation during all five Mock Elections, the procedural review focused on the first two attempts.

After several attempts at re-starting the process, resulting in increasing levels of vendor support, the stability of the system was deemed insufficient to complete the Mock Election, at which point PES finally conceded that programmatic changes to the applications needed to be made by their developers.

This section summarizes some of Anitian's observations and concerns that arose from the mock elections process.

4.6.1. Lack of Vendor Support

PES did not provide any on-site support for the first day of the first mock election. On the second day, a PES representative was on-site. Only after several failed mock elections and repeated demands from KCE did PES provide sufficient on-site resources.

4.6.2. Test Environment Not Exact Duplicate of Production

The mock elections environment was not an exact duplication of an actual elections environment. Only a few staff members participated in the mock election, and the testing did not emulate the actual intensity of a real time election. KCE performed a volume stress test during the end of writing this security report, which may help KCE evaluate the true performance of the system. However, those tests are focused mostly on system performance under heavy load, not procedures. Therefore, the procedures and security controls have not undergone the intensity of a full-scale election.

4.6.3. Variation From Acceptance Testing Plan

The Acceptance Testing metrics were adequate. However, the Mock Election did not follow some tests specified in testing plan. Anitian observed three areas of deviation from the test plan:

4.6.3.1. Adjudication of Ballots

> *"a. ix. Adjudication of ballots with a significant number of over votes, under votes, stray marks, and other anomalies normally seen on ballots returned by voters."*

During the Mock Election tests, very few ballots were designated for adjudication. These involved mostly blank ballots and over-voted ballots although there was a deck of ballots with stray marks and other issues. According to KCE staff, this limited number of ballots requiring adjudication was based on a recommendation from the Washington Secretary of State's Office.

KCE informed Anitian that a more strenuous test of the adjudication process was included in the Volume Test. Anitian, however, did not observe this testing.

Based on what Anitian observed, the adjudication testing appeared inadequate. However, if KCE did complete a more rigorous testing in the Volume Testing process (and that testing was successful), then there is no reason for concern. However, this still represents a deviation from the test plan and is worth noting.

4.6.3.2. UPS Testing

"a. xviii. During the process stage a power outage to test UPS sufficiency and determine run time available on current battery setup."

Anitian did not observe KCE conduct a complete UPS test.

4.6.3.3. Production Rates

"b. As part of the Acceptance Testing the following data will be captured

a. Capture production rates on new Hardware. This will be necessary in determining how County staffing levels will need to adjust with the implementation of the new equipment."

Anitian did not observe production rates being captured, although King County informed Anitian that production rate data was captured during the Volume Test.

4.6.4. Lack of Procedural Development

At the beginning of the mock elections, KCE stated that this effort would help develop final processes and procedures. However, Anitian did not observe a formal effort to do this. Notable examples include:

- The only procedures used were those prescribed in the vendor's User Manuals, which were clearly labeled draft. These were quickly found to be inaccurate, resulting in numerous ad hoc changes, additions and modifications.
- Changes were initiated in an inconsistent manner. Sometimes the vendor, or other times KCE, would initiate procedural changes. Often, these changes would spawn additional errors and problems, resulting in changes to the changes.
- Furthermore, Anitian recommended to KCE that a single person be identified as the official scribe (note taker) for the process. This person was to capture all feedback and notes. No person assumed this role. And while some KCE staff did take their own notes, there was no formalized process to capture this information and cohesively organize it.

Overall, Anitian did not observe a formalized effort to use the Mock Elections to evaluate and refine the processes and procedures.

4.6.5. Hardware/Software Integration Success Metric

The first success metric defined in the Acceptance Testing Outline is:

i. "All hardware and Software components required in order to conduct an election in King County function as Documented by the Contract, both individually and in concert with all other existing and new hardware and Software components, in a real election environment simulating a Primary Election, from the beginning of the elections process to final tally, accounting and certification."

After observing four failed mock elections and a final, fifth test that succeeded, Anitian concludes that while the Mock Elections did meet the most basic requirements of the test plan, KCE should conduct additional testing to ensure the stability of the environment in a "real election environment."

According to KCE, the Volume Testing did evaluate some of these stability issues. Nevertheless, additional testing is warranted, which KCE is already conducting.

4.7. Ballot Scanner Process Review

This section addresses the review of the PCS User Guide Ballot Scanning Process.

It is difficult to assess the operational security issues at this stage of election management. The user guide only describes how to get images scanned. It does not cover operational security issues.

King County needs to develop the operational protocols and processes that provide security for the ballots, system access and personnel involved in the scanning, adjudicating and tallying phases of the election.

As such, this section offers recommended improvements to the ballot scanning process that will help improve operational security.

4.7.1. Ballot Processing Log

This document is generated by the ballot processors. It currently only lists how many ballots are being sent for scanning.

This document needs to be re-designed so there is a paper record of how many ballots were scanned, how many failed, how many were sent to adjudication and any other anomalies that might occur.

4.7.2. System Authentication

Security tokens in conjunction with a secure PIN provide secure access to the PCS. The tokens are digital certificates stored on a smart card. This is generally a secure method, requiring two separate factors for authentication: something the user has (a physical token) and something they must know (a PIN).

However, there are no procedures for the management and accountability of tokens and PINs. These procedures need to be developed. They should include a complete inventory of all assigned tokens. Moreover, there should be formal methods to revoke, reprovision or reset tokens, particularly for recovery of critical tokens, like tally, during an election.

4.7.3. User Rights Provisioning

Scanning, deleting, adjudicating, committing and rolling back ballot scan batches are all assigned rights. Currently, there is no formal process for how these rights are assigned.

The best method is to establish roles. Each role has specific rights assigned to it. Users are then granted roles as part of a formal provisioning process. KCE needs to develop these processes, including how accounts will be deprovisioned upon employee separation, although this basic framework is already in use.

4.7.4. Ballot Flow Management

There are existing policies on how and where ballots are archived that are still viable. However, there are no policies on how ballots are handled throughout the elections lifecycle. Specifically, there are no formal policies for the following circumstances:

- Transport of ballots to the scanning room.
- Ballot storage within the scanning room.
- How and when sealed ballots are broken.
- Ballot handling after scanning.
- Ballot storage after scanning.
- Ballot storage while tallying.
- What data accompanies ballots after scanning.
- Determination of if ballots are re-sealed after scanning.

KCE needs to develop policies that address each of these points in a ballot's lifecycle. Ideally, this should be presented as a Ballot Flow. At each stage of the ballot's processing, there should be clear lines of authority and responsibility. When ballots are transferred from one person or group to another, there should be a structured, formal process that requires witnesses at every stage of the transfer.

4.7.5. The Commit Process

This is the process that allows vote totals to be tallied. This can not be done without a Commit Token and the appropriate permissions in the PES software. KCE has no formal procedures surrounding the creation, management and use of the Commit Token.

KCE needs to develop these procedures, which should specifically address:

- Who generates the commit token and when. It is acceptable to generate the token in advance, but if it is generated in advance, it must be stored securely.
- Where the commit token is stored until use.
- Who has permission to retrieve the stored token.
- Who will witness the creation and retrieval of the commit token.

Specific procedures for the management of the Commit Token need to be established to assure that no vote totals are viewable prior to 8:00 p.m. on Election Night.

This might involve creating the Commit Token in advance and sealing it in a secure area, or perhaps not even creating it until it is needed. Whatever direction is taken, the process needs to require multiple persons observing all creation, handling and use of the Commit Token any time prior to when results can be reviewed. contingency

4.8. Electronic Duplication Process Review

KCE has developed a "Draft" procedure for electronic adjudication of ballots using the new voting system (Ballot Resolution – Electronic Adjudication (MB2-002 A). Anitian reviewed this procedure in its draft form.

The content of the written procedure is appropriately based on existing sources that govern the duplication and adjudication of ballots, including the following document portions:

RCW 29A.60.125 Damaged ballots.

If inspection of the ballot reveals a physically damaged ballot or ballot that may be otherwise unreadable or uncountable by the tabulating system, the county auditor may refer the ballot to the county canvassing board or duplicate the ballot if so authorized by the county canvassing board. The voter's original ballot may not be altered. A ballot may be duplicated only if the intent of the voter's marks on the ballot is clear and the electronic voting equipment might not otherwise properly tally the ballot to reflect the intent of the voter. Ballots must be duplicated by teams of two or more people working together.

WAC 434-261-102 Agency filings affecting this section Resolving ballots on digital scan vote tallying systems.

In counties tabulating ballots on a digital scan vote tallying system, two staff designated by the auditor's office must resolve ballots identified as requiring resolution. A log of the resolutions must be printed and signed by the two staff.

Furthermore, the Vendor's User Manual, Section 7 (Premier Central Scan 2.2.1 User's Guide) contains the operational steps to adjudicate ballots in the system, although this document is also in draft form and is not sufficiently detailed for use in King County's operational setting.

From an operational procedure security perspective, it is extremely important for KCE to develop customized and detailed processes. Duplications, adjudication and determination of voter intent are complex processes that the public does not generally understand. Furthermore, it is an area of great concern for people worried about the possible manipulation of elections.

Since the new system is being implemented, it is important that these procedures are finished. The procedure and processes adopted should be very detailed. They should also assure the public KCE is being diligent and following effective security procedures. Each step at which a voter's mark is being evaluated, improved, accepted or rejected should be clearly explained and tied back to approved standards, following secure processes.

Anitian also suggests documenting this as a work flow. At each step in the adjudication process, there should be clear set of steps, expectations and oversight.

4.8.1. Recommendations

This section outlines Anitian's recommendations to improve the Duplication Process and procedures.

4.8.1.1. Additional Definitions Needed

In the Definition section, KCE should add definitions for "Adjudication Team", "Adjudicator" and "Interpreter". These terms are of primary importance, and while the duties are prescribed throughout the procedure, we believe they should be defined in this section.

4.8.1.2. Referenced Standards Should Be Added

In the Definition section, the defined term "opening pulls" references "Ballots the Canvass Board has determined they alone must rule on".

Add these standards to the procedure as an attachment and reference the attachment in this section. (Also see 3.8.6)

4.8.1.3. Disagreement Process Clarification

Sections 2 and 3 do not address what happens if the Adjudicator and Interpreter disagree on the resolution of a ballot. Section 4.0 addresses ballots "…required to be pulled and sent to the canvass board."; however there is no indication that Adjudication Team disagreement falls in this category; and if not, how this situation should be dealt with.

KCE should provide additional clarity on how these ballots should be handled.

4.8.1.4. Additional Reference Should Be Added

Items 2.0 11 a. and 3.0 9 c. should contain references to Section 4.0 such as "See section 4.0"

4.8.1.5. Define Opening Batch

Section 3.0 is titled "Ballot Adjudication – Opening Batch" however "Opening Batch is not defined. "Opening Pulls" are referenced in the definition section, but not "Opening Batch."

Add definition for "Opening Batch."

4.8.1.6. Add References to Adjudication Standards

While this procedure is adequate in identifying the specific steps operators must follow, it does not contain the standards that are used to determine how a specific vote should be adjudicated.

Since these procedures are likely to undergo great public scrutiny, KCE should reference the adjudication standards.

KCE should add a section that references the standards to be used. This should either be an appendix with the actual standard documents (preferred) or clear instructions how to obtain copies of the standards. The references should include:

- **Canvassing Board standards**. The standards that apply when a ballot is to be sent to the Canvass Board for review.
- **The Washington Secretary of State Publication: Voter Intent – Statewide Standards on What is a Vote, revised 2008**. This document illustrates, using pictures, how County Canvassing Boards should interpret ballots. This document contains information specifically related to digital scan ballots.

5. TECHNICAL REVIEW

This section focuses on Anitian's technical review of the PES voting software, hardware and operation. This section includes observations from the mock election as well as configuration analysis, threat modeling and penetration testing Anitian performed. Specifically, for each of the various components analyzed below, the following work order tasks (enumerated in section 1.2 above) were completed: 1, 2, 3, 5, 6 and 8. For all systems, extensive analysis and testing of the general security of the Windows operating system, such as the local security policy, Windows firewall and service configurations was performed, in addition to the Assure voting system components, which are discussed in detail below.

5.1. Mock Election Observations

As previously discussed, there were five total mock elections. The first four produced various software and hardware errors preventing them from completing successfully.

PES resolved most of the software errors after the fourth, failed mock election. The PES software underwent some bug fixes and new code was deployed for the fifth, and final, mock election, as well as for the volume testing.

5.1.1. Code Changes

As previously discussed, Anitian did not obtain information about the bug fixes and code changes until after the security review was completed and this report was scheduled for release. When Anitian obtained the bug fix report from PES, KCE requested that Anitian return and perform a complete validation of all documented changes. Anitian also was tasked to determine if any new bugs had arisen during the changes.

There was concern among KCE staff that the new code had not undergone sufficient regression testing. This was primarily due to the rapid release of the new code, as well as the fact that it still produced minor errors, including one that had been previously resolved. It is therefore reasonable to conclude that additional errors may arise during the first official use of this system. This presents a risk to KCE and the operational integrity of the elections process, and should be considered during contingency planning. However, based on Anitian's understanding of the volume testing and other functional testing KCE has planned, another Mock Election does not seem necessary.

Anitian reviewed 27 documented bug fixes: 14 for GEMS, 2 for the KCT, 4 for the ASS/ASM, and 7 for PCS. All of the fixes appeared to behave as documented in the development change log, which is provided as an Appendix to this document.

Anitian had specific concerns with the items discussed below.

5.1.1.1. 100090 - GEMS overwrites an existing database when a new database with same name is created

During the mock elections, there were numerous problems with GEMS and PCS that appeared to stem from GEMS having multiple databases with the same name. Each database is encrypted, with a cryptograph hash created for each, and displayed in GEMS.

Anitian confirmed that we were unable to create a new database with a duplicate name or load a duplicate named database. The nature of the workaround suggests that Assure is still using the database name as the identifier, rather then the hash. While Anitian was not able to directly exploit this, it would be preferable to identify databases with their cryptographic hash rather then their name.

5.1.1.2. 9814 - Table line draws over the 'number of under votes' text in SOVC report (GEMS)

The change log cited "*As 'Number of under votes' has been changed to 'No. of under votes', Now there is space between table line and column name.*" However, the actual text displayed is "NO. Of Under Votes" rather then "No. of under votes".

This may seem like a minor issue, but it is indicative of poor quality assurance practices. An effective QA process should have caught that the actual text cited in the bug tracking entry was not the same as what was actually displayed in the application. Anitian recommends the text be displayed as "No. of Under Votes" and not as documented.

5.1.1.3. 10073 - Allow users to specify database password at installation (ASS/ASM)

The change log indicates the following behavior should occur as a result of this change:

> *Users are now presented with a password screen after the activation screen. This password screen will allow them to specify a default password for the security service database, if none already exists. If, for some reason, a password exists on the destination machine, the installer will not display the password screen.*

This was confirmed to function as documented. The concern is that if a password exists from a previous installation, it must be known in order to use the new installation. Otherwise, the user will be locked out. If a password exists, users should be given the option to change the password.

5.1.2. Procedural Changes

Throughout the first four mock elections, PES made numerous procedural changes attempting to prevent further reoccurrence of errors. The procedural changes were made in an ad hoc fashion with little analysis of the consequences. These changes were also modified many times until the desired result was achieved.

It is understandable that procedures need to be regularly updated and optimized. But changing a procedure merely to compensate for software errors is not best practice, particularly without thorough regression testing of the impact of the new procedure on the operation of the entire system. While it is understood that many of the procedural workarounds were best effort attempts on the part of the vendor to mitigate the errors so that the mock elections could be completed on schedule, had they been thoroughly tested rather then delivered to the customer in draft form, perhaps many of the delays could have been avoided.

5.1.3. Acclimation to the System

Anitian observed that staff took some time to become acclimated to how the PES software and hardware worked.

For example, a KCE staff member that was not part of the acceptance testing team helped during the one of the mock elections. The staff member had received some basic training on Assure, mostly focused on scanning of the ballots. When the scanner failed to scan a ballot properly, due to jamming or double picking, it was not clear to the user if the ballot was or was not counted. In this incident, three of the twelve decks that were scanned, came out with less ballots scanned than were in the deck. As such, the entire deck had to be rescanned. This is a failure rate of about 25%, which in a full scale election would result in a large number of decks having to be rescanned.

While there are procedures in place to ensure that the ballots are actually counted, this failure rate can lead to some rather significant operational inefficiencies.

Furthermore, the person who was performing this role during the mock elections was a full-time elections employee with a good understanding of the overall elections process and issues. During an actual election, temporary staff would be used to perform this scanning. This underscores the need to train all temporary staff on how to properly scan decks and follow established procedures. In discussing the results of the volume testing with KCE, which included users who were new to the system, the same issue was observed to occur, but with a reduction in failures over the course of the week as the users acclimatized.

5.1.4. Errors Reported

The following table lists the errors that were reported during the mock elections.

After the fourth mock election, PES released new software to KCE, with a second release after the fifth mock election, for the volume testing. This software fixed a number of bugs, although new bugs were introduced, as well as older bugs reemerged. The errors observed before the emergency releases are listed below, as well as the errors observed during the volume testing, which are noted as such.

#	Description

1. On the ASM server, the directory `C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA` was being populated with millions of encryption keys. At first PES stated that was expected behavior of MS Cryptographic services, before acknowledging the behavior seemed unusual and that they were not sure of the cause. This bug was ultimately fixed in the new code released after the fourth mock election, and appeared to be an artifact of the SSL handshake used by DTNP.
2. PCS would occasionally freeze, requiring terminating the process using the Window task manager. This occurred numerous times, often when trying to authenticate the user's security token on the smart card, as well as after scanning a deck. It also happened when trying to connect to the Tally Net, with audit log entries being created that stated "The operation failed because the scanner driver is not open. Not all scanner settings could be applied." Other times PCS would crash with no error message at all, or sometimes with a pop-message that a debugger could not be found.
3. Scanner LCDs displayed hardware errors, often while sitting idle. Cycling the power generally worked, although occasionally there were errors with PCS restarting after the failure that required files to be deleted by administrators, e.g. An error message from

#	Description

PCS that the system.adt log could not be found, even though it existed on the file system. Often times the scanners required diagnostics and recalibrating, and would also commonly lose their ballot sorting profiles.

4. PCS reported a "SQL Logic Error" on then adjudication workstations when trying to open a workspace, because it lost track of the state of the runs on the Tally Net. Changing to the current run allowed the vote center to be activated without problems.
5. PCS would sometimes report a workspace as being locked, even though it was closed on all Tally Net nodes. The workspace could then not be edited, nor it's token retrieved. Sometimes rebooting would solve these problems, but in other instances the workspace could not be recovered.
6. Adjudication workstations would freeze while attempting to synchronize with the Tally Net, as indicated by the green status bar, which would never completely fill in, preventing them from being adjudicated.
7. There were various hardware errors with the scanners not reading ballots properly, such as not displaying the marks in the circles but in the text elsewhere on the digital ballot images. Other common issues were the printing of a vertical pink line down the length of the digital ballot image, which would occasionally run through the vote circles, as well as stretched ballots due to them not being fed though the scanner at the correct rate. Often times these ballots were not being rejected as expected for rescanning, but instead sorted to the "needs adjudicated" tray, resulting in a long, tedious manual adjudication process. Ultimately, they had to delete the batches and rescan them because tabulation numbers didn't match up.
8. Attempting to scan a deck a second time was prevented as expected, but subsequently TN showed a bunch of spurious entries for that deck number, with the station ID listed as various binary characters and DCOM strings. These decks were unable to be deleted from the remote or local workspace. PES originally felt that KCE was not following the proper scanned procedure, until their demonstration to KCE staff on the correct sequence of actions resulted in the same error. At this point they acknowledged it must be a software bug, and this was ultimately the error that caused the stand-down of the acceptance testing to occur so that PES could address the numerous system errors.
9. Error observed during the volume testing - On one adjudication workstation, the workspace has become corrupted and will not load. Similar errors were observed before the bug fixes, but were much more prevalent.

10. Error observed during the volume testing - Temporary files are not being deleted automatically by PCS from C:\Documents and Settings\All Users\Documents\Premier Election Solutions\PCS22\Cache|Downloads|Temp|Uploads. This is something that happened before was fixed before and has remerged. As a work-around for the

#	Description

volume testing, KCE wrote a script to delete them. At first, the scrip ran at the end of each night, but KCE quickly realized they needed to run the script twice a day to avoid running out of disk space.

11. Error observed during the volume testing - Some ballots have been incorrectly scanned.

    In one instance, PCS appears to have merged the top ½ of one ballot with the bottom ½ of a second ballot into a single image. The combined image was accepted by PCS, and the only reason it was even noticed was because of one particular race had a vote filled in that resulted in an over-vote and required adjudication. From the adjudication screen, the operator realized that the race on the image did not correspond appropriately. Had the one race not had the particular candidate selected, this ballot would have been incorrectly accepted with a vote for the wrong person. PES has declared this case to be an anomaly.

    In the second instance, another ballot image had the front of one ballot stored as the front, but then the front of a second ballot stored as the back of the image. This resulted in PCS flagging the ballot for adjudication. KCE was unable to reproduce this error by gluing the same two ballots together in any combination of orientations and getting PCS to accept the scan, and PES is not sure what caused this error.

5.2. General Threats

This section is an assessment of the threats to the entire tabulation environment at KCE, rather then specific components, which are discussed in greater detail below. For issues that apply to more then one of the applications in the Assure voting system, the group as a whole is referred to as Assure.

It is important to consider individual threats in regards to the entire security posture of the KCE tabulation environment. There are technical security controls in the network architecture that mitigate some of the general risk to penetration of the network.

The primary strength is that the environment is running on a closed network, which is not connected to the internet of other business systems within KCE. There is no public access, physical or otherwise, to any of the systems other then the AVUs. Therefore, the primary threat agents are malicious insiders. This is why procedural controls, proper vetting of the users, and physical access control are so important.

Assuming a threat agent was granted legitimate access to the system during an election, they would be generally limited to the user interface (UI) of the applications and operating systems for any type of election manipulation or corruption. Physical access control to the USB and CD trays of the scanner workstation are protected with security seals to prevent them from being used to upload software without being noticed. The security seals are touch-sensitive, and display a Void watermark to indicate when they've been broken or removed. There is a barcode and number on them that is tracked in a master spreadsheet, and they are validated before each use of the systems to ensure they have not been replaced.

The network switch is well secured. All inactive switch ports are disabled, and the active ports are bound to the media access control (MAC) address of the allowed system's network interface card (NIC). The MAC addresses are not visible from the outside of the scanners for easy MAC address spoofing. Also, all workstations and servers use the Windows firewall, which provides additional host-based access control.

5.2.1. Third Party Software Uses Older, Deprecated Versions

Risk: Medium

Assure uses several different third party applications to provide functionality to their various products. The following four applications were found to be behind their current release. Some of these older versions have well known software bugs and vulnerabilities. While there are currently no severe exploits, there are some moderate risk vulnerabilities in the version of OpenSSL in use, and there is no reason to assume that more severe vulnerabilities will not be found in these deprecated versions future.

Name	Description	Version in use	Version date	Current version
Libpng	PNG image processing library	1.2.8	2004-Dec-3	1.2.34
Libtiff	TIFF image processing library	3.8.0	2005-Dec-12	3.8.2
SQLite	Embedded database engine	3.3.6	2006-Jun-6	3.6.11
OpenSSL	SSL communications library	0.9.8g	2007-Oct-19	0.9.8j

Recommendation

All 3rd party software should be updated within Assure whenever new versions are released, so that publically disclosed bugs and vulnerabilities within those programs cannot be exploited or otherwise degrade the operation of Assure. It is understood that the software cannot be patched after it has been certified. However, these should have been updated to the latest versions before submitting the software to the EAC. In some cases, the versions in use are much older than the last certification.

5.2.2. Windows Hosts Insufficiently Hardened

Risk: Medium

There has been some basic hardening of the Windows hosts as directed by the Vendor in the various administration manuals for the applications in Assure. However, there are some additional steps that should be taken to ensure integrity of the systems.

Recommendations

Comprehensive hardening recommendations are included as an appendix. KCE should evaluate these and consider implanting them as they deem appropriate. It should be noted that these reports were run on the final build of the lab machines. Anitian observed minor discrepancies between the final test and production environments, but was not permitted to run software on the production environment. PES was responsible for maintaining both environments.

Anitian used Center for Internet Security's (CIS) Scoring Tool, which is available at http://www.cisecurity.org. The CIS is a non-profit organization that provides technical benchmarks and scoring tools for a wide range of common network devices, operating systems and applications.

Additional resources include federally provided security checklists and templates, such as those provided by DISA (http://iase.disa.mil/stigs/SRR) and NIST (http://checklists.nist.gov). Anitian recommends leveraging at least one of these resources to ensure uniform security hardening of all hosts on the Assure network, meeting or exceeding best practices.

5.2.3. Windows Firewall

In the Windows firewall, programs are added to the *Exceptions* list so that the various components of Assure can communicate. However, their scope is set to allow communication to any computer, and should be restricted to an explicitly defined list of hosts on the Tally Net for each exception. Additionally, security logging should be enabled.

5.2.4. Incomplete System Documentation

Risk: High

There were numerous errors throughout the draft documentation for Assure that were discovered when attempting to set up the environment following the instructions.

Recommendations

KCE has started writing their system documentation to augment the insufficient material provided by the vendor. Anitian agrees with this response.

It is critical that these procedures be completed in great detail, and be thoroughly tested to ensure their accuracy, so that configuration errors do not interfere with the operation of Assure.

Lastly, KCE should ensure that deliverables, particularly support and technical documents, have clear deadlines and expectations. PES demonstrated a tendency to delay delivery of documentation until the last minute. This suggests a pattern of ambivalent support for KCE.

5.2.5. Critical Windows Patches Not Applied in a Timely Manner

Risk: Moderate

Because the system must be frozen on the date of certification, Windows patches can not be applied, which come out on at least a monthly basis. The system could be exposed to any number of vulnerabilities, such as privilege escalation, unauthorized code execution and others.

Recommendations

The Secretary of State should allow the most critical operating system and supporting application patches to be applied. However, these patches and updates should undergo extensive regression testing to ensure they do not break application components.

For the case where patches are released after the logic and accuracy (L&A) test is completed and the environment is "locked down" for an election, patching can be delayed until after the election. If KCE decides that the patch must be implemented before the election, then the L&A testing should be repeated after the patch is applied.

Contractual language should require Premier to review all patches on a regular schedule and provide KCE with guidance on which patches can be applied to the Assure environment and any ramifications from those patches.

5.2.6. Network Time Protocol (NTP) Service Not Running

Risk: Moderate

The network time service can be run on the domain controller or switch in order to synchronize the clocks on all network hosts. This ensures that all audit log timestamps are synchronized and enable events to be traced through across the network with increased assurance.

Recommendations

Run NTP and synchronize clocks on all network hosts.

5.2.7. Insufficient Event Log Collection

Risk: Moderate

There are several different logs used to collect events through Assure, as well as the various Windows system logs. Due to some of the issues discussed in this document, including various attack vectors and software bugs, there is the potential for these logs to be lost, corrupted or tampered with.

Recommendations

All logs should be identified and achieved to a central log server in real-time, or as close as possible, to ensure their integrity.

5.2.8. Windows Security Polices Distributed by a Third Party

Risk: Moderate

PES instructions require that security policies be downloaded from Microsoft for host hardening. However, Microsoft may change security policies with adverse consequences to the operation of the system. This may immediately result in the system not operating correctly. It could introduce more subtle problems that may corrupt the general operation of the election system in a manner that is not obvious to the system user.

Recommendations

KCE staff should not be directed to a third party for distribution of security policies to apply to the Assure environment. KCE should require PES to develop and distribute their own security policies for the Assure systems, following the recommendations in section 4.2.2 above. This should ensure that all policies are thoroughly tested for compatibility with Assure.

5.2.9. Untrusted Publisher Security Warning Displayed when PCS Runs

Risk: Low

This could condition users to expect warning, leading them not to notice if the software publisher (digital certificate) has been changed, which could be indicative of malicious software.

Recommendations

Install the "Premier Code Signing Authority" digital certificate as trusted publisher to all Windows hosts so that a warning doesn't appear each time the application is run. The Premier Root CA should also be uniformly trusted by all network hosts (e.g. it is a Trusted Root certificate on ASM, but not on GEMS).

With these trusts in place, users can then be trained to report any security warnings, thus preventing malicious code from being run.

5.3. Accessible Voting Unit Threats

When analyzing the AVU's, Anitian conducted a series of tests to check the integrity of the system and the memory cards. Anitian attempted to perform the following tests:

- Tamper with the election database file
- Alter votes recorded to the memory card
- Alter configuration files
- Tamper with encryption keys
- Crack encryption mechanisms
- Inject malicious code into the AVU
- Attempt to install hacking utilities to the AVU or use the AVU as a launch pad for attacks to the GEMS application.
- Upload a fraudulent memory card.

In most cases, Anitian's attempts to tamper with the AVUs were unsuccessful. However, a few tests did yield some potential risks. KCE has implemented mitigating controls to physically secure the unit's hardware for subtle or undetected tampering. This section itemizes the threats that Anitian was able to identify.

It is important to note that the AVUs have numerous physical and procedural controls that very effectively mitigate some of the threats described in this section. For example, the AVU memory cards are locked into the cases. The locks are protected with tamper evident stickers. Each sticker has a unique serial number which is recorded and validated when units are sent out and when they return. These controls, as well as other procedural controls in use at KCE, would make it very difficult for an attacker, either internal or external, to carry out a successful attack against the AVU memory card. Nevertheless, these threats are real and there is no reason they should not be addressed.

5.3.1. Memory Card Tampering – Redirect Results To an Incorrect IP Address

Risk: Low

Anitian conducted a series of tests against the AVU memory cards. The memory cards are standard PCMCIA cards that can be read with any standard PCMCIA reader. Anitian used an off the shelf Dell laptop with a PCMCIA slot to conduct these tests.

For this test, the host entry in the election.ini file was modified to point to a different IP address. Anitian then set up a listening host on the IP address we placed into the .ini file. When the card was placed into the AVU it successfully read the card and reported no errors. When Upload Results was selected, the AVU connected to the IP address Anitian had maliciously set in the .ini file. Based on this, a malicious hacker could possibly force an AVU to send results either to another GEMS host on the TN under their control, or simply dump the results to a non-existent host so that they don't get recorded.

The impact of this risk is mitigated by the fact that only the AVUs in the tabulation environment are networked.

Recommendations

The files on the AVU memory card are not being properly digitally signed. The files are signed, but apparently the entire file is not being signed or no integrity checking is being performed.

As such, when a file is changed, the AVU is still accepting the modified file.

Digital signatures and hashing is apparently already in use. Some of the tests Anitian performed did cause the integrity checking to fail. As such, it seemed that only portions of the file were being hashed, not the entire file.

KCE should require that all files on the memory card are completely hashed. And any changes to the files since creation should result in an AVU error and notification to the operator that there is an error.

5.3.2. Memory Card Tampering – Instruction Modification

Risk: Moderate

The next AVU memory test was to the text instructions that are displayed to the user. These are stored in a .xtr file on the memory card. Anitian modified this file offline and then placed the card into the AVU. The AVU accepted the card and displayed the modified text.

In our test, we specifically changed the instructions to direct the user to a selection that would be the exact opposite of their intent (a statement referring to an action resulting in ballot being cast, to not being cast.)

In this specific instance, a user could be duped into thinking their vote had been casted, when it in fact had not been. However, there was a large amount of instructive text that could have been modified with various outcomes, all of which would potentially corrupt the integrity of the votes cast on that card.

Recommendations

This item has essentially the same recommendation as the previous threat. All files on the memory card should be completely hashed. Any changes to any files should result in an error and alert the operator to the integrity failure.

However, the Logic & Accuracy testing would detect these tampering attempts. As such, the likelihood of this risk is significantly reduced.

5.3.3. Memory Card Tampering – Script Injection

Risk: Moderate

Anitian was able to create additional files on the AVU memory card. For this test, an accubasic object script was placed on the card. These scripts are a proprietary symbolic language that GEMS uses.

Anitian was not provided information about the AccuBasic language or a copy of complier, as analysis of this language was beyond the scope of this assessment, and has been performed by other states. However, a threat agent with an understanding of the language may be able to create a script that could inject malicious code into the AVU by adding it to the memory card. Injected code could potentially perform any kind of malicious activity, including dropping votes, changing records, or corrupting data.

Recommendations

Same as above, all files on the AVU memory card should be hashed. Any changes to any files – or the addition of any unauthorized files, should cause the AVU to fail and the operator to be alerted to the integrity checking failure.

5.3.4. Memory Card Tampering – No Audit Logs

Risk: Moderate

The AVUs generated very few useful audit logs. The only logs Anitian detected were from failures to upload results to GEMS. For example, the previously mentioned IP address redirection threat generated a log entry for a failed upload.

There were entries showing the audit log being moved and synched with the backup copy on the machine after we had modified them on the card. However, the log listed no explanation of why.

When Anitian attempted to tamper with the election database file (.edb), this caused the AVU to display "Unable to load the election: the election database appears to be corrupted.", although an audit log entry was not generated.

Recommendations

Audit loggings need to be more verbose, which must be implemented programmatically by PES. In the interim, all existing procedures concerning the AVUs and Memory Cards must be rigorously adhered to. Additionally, procedures should be monitored to require all elections staff responsible for using the AVUs to manually record all events that are displayed on the screen, as they are not all added to the audit log (such as the AVU being unable to load the election on the memory card due to a failed integrity check).

5.3.5. Dedicated Workstation for Encryption Key Generation

Risk: High

The KCT is a program PES provides to change the encryption keys that GEMS and the AVUs use. Changing these keys is important, since the defaults are widely known.

Protection of encryption keys is vitally important to maintain the integrity of the encryption. If a malicious user is able to steal encryption keys or generate fraudulent keys, then the entire integrity of the encryption is compromised.

For the new environment, this is performed on the regular workstation of one of the KCE IT staff members. In the current environment, a dedicated laptop is used. However, this laptop is left in plain view and has authentication credentials written on a post-it note attached directly to the laptop.

This is a very serious breech of physical and basic security controls. Since the workstations are neither physically secured nor used for general computing activities, there are numerous potential vectors for a determined hacker to gain control and tamper with the generation of the encryption keys.

Recommendations

The KCT should be installed on a dedicated workstation and or laptop. This system should be kept in a secured location, with no internet access.

Additionally, the hard drives in these systems should be completely encrypted to prevent theft of the hard drive or forceful removal of the keys.

USB, CD and all other communication and/or media ports should be disabled on this workstation or laptop. If possible, these should be physically secured as well, such as with the security seals used elsewhere in the Assure environment.

There should be only a few authorized users and each person should have their own logon credentials. All logons to the system should be recorded in the windows event log.

Users should be required to remember their passwords and forbidden from writing them down.

A witness should be present whenever encryption keys are generated. All keys should be stored on this secured system and on no other media.

KCE policies and procedures should be updated to reflect these requirements.

5.4. PCS Threats

When analyzing PCS, Anitian conducted extensive security analysis and testing, based on the work order components listed in section 4 and enumerated section 1.2 above. All aspects of the PCS application were tested, including an extensive review of the audit logs.

Anitian also performed tests based on the issues listed in the Humboldt County report. However, the KCE environment is different from Humboldt County. Humboldt County is running older versions of GEMS and KCE does not use a central count server to tabulate OS ballots. Nevertheless, Anitian tested these issues anyway, to ensure they did not cause an issue with PCS.

Anitian also analyzed the Distributed Tally Net Protocol (DTNP) used by PCS to synchronize the Tally Network. Anitian made numerous requests to KCE and PES for documentation on the DTNP. PES told Anitian that such documentation did not exist and that the development team did not have time to produce documentation on the DTNP.

To analyze the security of the DTNP, Anitian performed network packet captures on the network and analyzed the components of the DTNP. The protocol appears to use DCOM and HTTP, and the data in the packets is obfuscated from plain view. Anitian was not able to decrypt the traffic.

PES did not supply documentation on DTNP to Anitian until after this report was scheduled for delivery. KCE extended the deadline so that Anitian could review the report and other information provided. DTNP is in fact using a version of HTTP. Data is encoded using the Tiger-tree hash algorithm, rather then a traditional one-way hash such as SHA-1 or MD-5, due to the distributed nature of the TN data. However, the published cryptanalysis of the algorithm does not reveal any notable weaknesses. Encryption is supported using AES, which is a best practice, but is not applied to all data. The protocol specification goes into some depth explaining why all data is not encrypted. The overall reason cited is because the data is displayed in plain text within the application. This overlooks the point of encrypting data in transit, which is to prevent eavesdropping or manipulation.

Nevertheless, since KCE's environment is completely closed and locked down, such interception and manipulation is highly unlikely. The protocol specification clarifies which data is and is not encrypted as follows:

> *The Central Scan application does not encrypt base workspace information, since the data is already encrypted at its source and can simply be transmitted in its native form without redundantly re-encrypting it. For ballot box data dynamically generated through the processing of ballots (e.g. deck lists, deck contents, scanned image data, etc.), that data is encrypted for export at the source machine and transferred encrypted to the requesting client node. Encryption for transfer purposes uses symmetric 128-bit AES and/or RC4 encryption (although the specific algorithm and block size is technically configurable in the application and additional/alternate algorithms may be used in the future) using key data derived from the sign on associated with the corresponding database in the ASSURE Security Service.*
>
> ...
>
> *It should be noted that only election data is encrypted for transfer. HTTP request and response headers are not encrypted, per the protocol specification. Similarly, DTNP backbone/infrastructure messages are not encrypted either since there is nothing sensitive to hide in the messages passed via that aspect of the protocol.*

The vote center files that tally votes use an .edf extension. This is a Microsoft Access database file format. Anitian was unable to open this file in Microsoft Access. When the file was opened with a hex editor, the data was unreadable. According the PES representatives, these files are encrypted using a proprietary format. Access limits the size of these files to no more than 2GB. However, the software places them into separate, compressed folders to limit the size of the files.

Anitian also conducted numerous stress and tamper tests to the operation of PCS itself, in regards to deleting decks, trying to change workspace settings, and so forth. Many of these were iterations of mistakes made during the initial operation of the software or procedures that resulted in software errors.

In most cases, the system responded positively and prevented Anitian from tampering with data or gaining unauthorized access. However, there were some threats identified that deserve attention. This section itemizes those threats and the risk they pose.

5.4.1. Weak Workstation Authentication Measures

Risk: Moderate

Smart cards are used to logon to each PES workstation. This is a good design and provides strong authentication. However, the smart card is only required for authentication. Once authenticated, the card can be removed from the reader and used in a different workstation. This would allow a user to logon to multiple workstations simultaneously and thus share authentication credentials.

Recommendations

Ideally, the application would require that the smart card remain in place for the entire session. Removal of the card would immediately lock the workstation. However, because the user token must be removed for the insertion of the commit token, this would not work with the current architecture. KCE and PES should evaluate this issue and determine if there is a way to improve this process that would still require the user to keep their smart card in the reader during their session.

Moreover, users should be prohibited from logging on to multiple workstations. If they are logged into one workstation, any attempt to logon to another workstation should fail, or the other session should be terminated.

Audit logs should reflect all logon and logoffs as well as any attempt to perform a multiple logon.

KCE should modify policies and procedures to require users to keep their smart card inserted into the reader during their entire session. If a user leaves the workstation, they should be required to take their smart card with them.

5.4.2. Required Cards Are Not Enforced

Risk: Low

This bug is not a specific threat, but is a prime example of how changes made to software can result in all sorts of unintended consequences. It is clear that PES did not perform sufficient QA on the software before it was presented to KCE for deployment.

In the Control Card Profile of the Vote Center Settings, there are settings to define which control cards are required. Per PES instructions, KCE was requiring a Deck Ender Card.

However, during the mock elections KCE was not using Deck Ender Cards. KCE staff was able to close decks in the PCS application. The control setting is the default, along with Deck Header cards.

After the GEMS software was updated during the first bug fix release, the Deck Ender entry in the GUI was instead a duplicate entry of Deck Header, and Deck Ender could not be selected. This was pointed out to PES and they agreed that it seemed to be an error that could not be explained.

Recommendations

If cards are required to complete certain tasks, that should be enforced in the application. KCE should require PES to repair this specific bug.

Moreover, as previously described, KCE should require PES to complete comprehensive regression testing of all software components before any new or updated software is deployed.

KCE should also perform acceptance testing of any new PES software before it is used in production.

5.5. GEMs Threats

When analyzing GEMs, Anitian conducted extensive security analysis and testing, based on the work order components listed in section 4 and enumerated section 1.2 above.

For these tests, no deficiencies were found that were specific to GEMS. In addition to the general testing, the ability to open the GEMS database in Microsoft Access or view the election data in another software program such as a hex editor was tested. The files could not be opened in Access and were obfuscated when viewing them in other software.

Additionally, Anitian reviewed the deficiencies that were reported in the California State Review. The two most critical deficiencies from the California report have been fixed: 1) the clear button from the audit log has been removed and 2) the "deck zero" flaw could not be reproduced in the KCE environment.

However, there was still some concern with the deletion of decks and audit logs, as well as the audit logs themselves. The threats are listed in this section.

5.5.1. Decks and Audit Logs Can Be Deleted

Risk: Low

The normal behavior for KCE is to upload results of a tallied run to the AVServer on GEMS.

However, it is possible to start the Central Count Server (CCS) in GEMS, which KCE is not using, and view the decks that were uploaded to the AVServer. Through the CCS, a user can delete any deck from the final tally, without any type of warning or prompt for confirmation. The CCS audit log (cclog.log) does record this deletion occurred. However, this log can be easily edited in any standard text editor. As such, a malicious user could:

- Start the CCS and select the Decks tab.
- Delete one or more decks.
- Shut down the CCS.
- Open the cclog.log file in Notepad (or any other text editor).
- Locate the log entry that indicates the deletion.
- Remove the log entry and save the log file.

At that point, there would be absolutely no record of the deletion.

However, records of the run still exist in PCS. If PCS is still connected to the AVServer, then it will resend the deleted deck upon the next synchronization. If PCS has been disconnected from the AVServer on GEMS, the deck would not be resent, resulting in the votes in that deck from not being recorded. However, due to the strength of KCE's existing controls, such as their validation routine, the missing deck would very likely be noticed. As such, the likelihood of this threat actually happening is quite low. Nevertheless, the impact of such a threat would be quite high.

Recommendations

There are already some mitigating, procedural controls that reduce the probability of this threat from occurring. Nevertheless, the impact of this threat is extremely high and therefore the risk warrants remediation.

KCE should develop additional procedural controls to ensure that GEMS server access is very tightly controlled. GEMS server access should always be supervised. All actions should be carefully monitored.

Moreover, KCE should require PES to reconfigure the GEMS server such that logged on users cannot modify the cclog.log file. Alternatively, these logs should be kept in encrypted, format that only an authorized application can read.

5.5.2. Encoded Timestamps

Risk: Low

In the GEMs audit logs, the timestamp format is unnecessarily arcane. Events are recorded using a UNIX timestamp format. This format is based on seconds since standard epoch of 1/1/1970. Most people are not familiar with this format and cannot read it. It also seems counter-intuitive for a program running on Windows to use a UNIX timestamp format, when Windows supports standard timestamps. This format could hamper troubleshooting and incident response. Users would need to decode the timestamp to evaluate events.

Recommendations

KCE should require PES to change the audit logs to use normal timestamps, consistent with the rest of their product suite.

5.6. ASM Threats

When analyzing the ASM, Anitian conducted extensive security analysis and testing, based on the work order components listed in section 4 and enumerated section 1.2 above. In most cases, the ASM responded positively and prevented Anitian's attacks. However, threats were identified. This section outlines those threats and the risk they pose.

5.6.1. ASM Logs Lack Detail

Risk: High

The current ASM logs do not provide sufficient detail of changes and modifications made, and there is no way to increase the verbosity of the AMS logs. For example, any changes to a user's profile result in an entry such as *updated user scanop1*. There is no indication of what was changed, such as permissions being granted or removed. Also, there are Event ID numbers, but there is no information provided on what they mean in the application's documentation.

Recommendations

KCE should require PES to increase the verbosity of all logs such they indicate exactly what change was made and by whom. Ideally, the verbosity would be able to be set by the administrator through the GUI.

Furthermore, KCE should require PES to provide documentation on what each event ID number means.

Procedurally, KCE should ensure that at least two employees are present anytime changes are being made to the ASM, and that manual logs or notations are made of all changes, since the ASM log is incomplete.

5.6.2. ASM Token Pin Creation is Displayed in Plain Text

Risk: Moderate

When creating a user's pin for their security token (which is stored on a smart card in the KCE environment), the pin is displayed on the screen in plain text. This is not best practice. It allows any eavesdropping of the PIN from onlookers.

This risk is listed as moderate since the probability of exploiting this would still be very difficult, since an attacker would still need a user's smart card. However, because the smart cards are not required for operation of PCS, only identification and authentication, there is an increased likelihood that a user's smart card could be temporarily stolen without them being aware.

Recommendations

KCE should require PES to fix this aspect of the application to obfuscate PINs as they are entered. The standard method is to display asterisks as the PIN is entered.

There is no technical mitigation for this risk other then having the vendor provide programmatic enhancements to the application. Procedurally, KCE should ensure that the creation of users through the ASM is done in a private area, with the monitor positioned in such as way that other people in the room cannot view the pin when it is being created.

5.6.3. ASS is Running as Local System.

Risk: Low

Services should always run with dedicated accounts with the least privileges necessary to operate correctly. This limits the scope of any attack, if the application is compromised.

Recommendations

KCE should require PES to reconfigure Assure such that all services run with dedicated Windows accounts. Those accounts should only be able to access the areas of the computer that are required for the services operation and nothing more.

Furthermore, KCE should require documentation from PES to define the rights granted to the service accounts.

5.7. Photoscribe Scanner Threats

The Scanners are controlled through the PCS interface. KCE testing is described in section 4.4 above. In addition, a physical security assessment was performed, which validated that KCE has sufficient mitigating controls for hardware tampering, namely the security seals and building access controls.

This section itemized the threats that Anitian was able to identify from our testing.

5.7.1. Hardware Failures Caused Sorting Profiles to Be Lost

Risk: Low

It was not uncommon for the scanners to experience various hardware errors, or PCS to lose communication with the scanners. Rebooting the scanners usually fixed any problems. However, when the scanners were rebooted, they would often lose their sorting profiles. This would cause ballots to be scanned after the reboot to be incorrectly sorted.

Another problem was that the loss of the sorting profile would cause the scanners to lose their orientation settings. However, this would prevent ballots from being scanned and as such did not introduce any additional threats.

Recommendations

When the policies and procedures for scanner operators are written, as previously recommended, they should include the requirement that operators check the settings of the scanners in PCS anytime there has been a recovery from a hardware error.

5.7.2. Loss of Configuration Key When Units Are Repaired

Risk: Low

By design, anytime any of the moving components in a scanner are replaced, the licensing keys must be reinstalled. These keys are only available from PES or the manufacturer.

If an election is in progress, and a large number of scanners need repair, this could lead to numerous scanners being permanently offline if the keys could not be obtained, even though the hardware problem has been repaired.

Recommendations

At a minimum, KCE should establish a formal process to retrieve keys from PES or the manufacturer each time a scanner has a hardware repair, and contractually define their availability through a service level agreement (SLA).

Ideally, PES should provide a copy of all keys to KCE. Those keys should be stored in a secure location.

6. CONCLUSION

Anitian has performed a comprehensive security review and threat assessment of KCE's election environment, process, and Assure voting system. This assessment was based upon observations, tests and data collected. No part of this assessment is based on personal opinion or conjecture, rather observable facts and empirical evidence.

While numerous technical and procedural risks exist, it is Anitian's assessment that with the proper controls and procedures, many of these risks can be reduced to a reasonable level such that the overall environment can support the secure execution of an election.

To summarize, the answers to the questions from the work order, requiring specific security features or potential vulnerabilities of the system will be evaluated:

Question	Response
Is the encryption of the database implemented in a secure way and in such a way as to make meaningful manipulation of the database impossible?	Yes. It would be extremely difficult if not impossible to manipulate the data in the database as it is stored.
Can the database be accessed outside of the GEMS or CTS system?	The databases for the various CTS components are files that reside on the Windows file system, and as such they can be accessed and copied. However, they are encrypted and are furthermore in a format that is no longer recognized by Microsoft Access.
Are the program certificates of authentication implemented such that the certificates can be trusted to ensure application programs in use are the original unmodified federally certified applications?	The framework is in place for this, but the certificates are not trusted by the workstations that run the applications. Anitian provided recommendations to mitigate this issue. Furthermore, KCE's procedures use a separate tool to hash the applications.
Can the results from a ballot that was electronically duplicated be manipulated outside of the CTS application?	No. Ballot images are stored in a protected database.
Is it possible to preview cumulated election results within or outside the system going around established procedures and if all security features (including smart card technology) are properly implemented?	No. Provided procedures are followed properly, this should not happen.

Question	Response
Is the database replication among scanner units performed in a secure manner?	It appears to be, in regards to confidentiality and integrity, based on Anitian's analysis of the protocol and use and the specification provided by PES. However, there were numerous deficiencies with replication of the ballot scan data that appears to have remediated after the emergency bug fixes, but could impede the availability of the database on the TN.
Is application level access control performed by the security module adequate – can rights, privileges, use of smart card, etc…be bypassed or escalated outside of the application?	The application access controls are sound. Anitian was unable to perform any kind of privilege escalation within the CTS. There are deficiencies in the security posture of the Windows operating system that should be corrected to prevent attacks on the operating system access control.
Are the scanned ballot images stored securely? Is it possible to access ballot images by bypassing any security controls?	Ballots images are securely stored in the workspace database and could not be accessed outside of the applications. Furthermore, they are encrypted during transfer across the TN.

Sound procedures and practices can compensate for software weaknesses and mitigate risks. But the existence of those weaknesses still demands correction. KCE has many sound practices and procedures, but there is room for improvement. Furthermore, KCE needs to work with PES to correct outstanding problems mentioned in this report.

Anitian is ultimately confident that KCE can operate this system in a secure and reliable manner.

APPENDIX A – BUG FIX LIST

PES provided the following list of bug fixes to Anitian. The list is presented exactly as it was provided from PES.

GEMS 1.21.2 to 1.21.3
10049 Update GEMS 1.21 Comma delimited ASCII Export
10064 Add activation code and certificate installation to GEMS installer
9954 Ballot Text Preview window clean up
9961 Poster window should be extendable
9970 Allow override of connection timeout with registry entry
10009 GEMS overwrites an existing database when a new database with same name is created
10053 Log failed user login attempts
10089 Enhance GEMS Poster log messages
9836 Revisited # 1521: View Ballots does not correctly reflect candidate choices if a race marked 'not counted' includes cross-endorsed candidates.
9988 GEMS Exception error occurs when linking Preference race to Voter Group 2. Voter Group 2 menu should be grayed out with <N.P> when Race type Endorsement is selected.
9801 Non-descriptive error message is displayed after ballot layout if a race has no RTF text or candidate.
9966 Change 'Show Non-Voted Candidates' label to 'Print/Export Non-Voted Candidates'.
9814 Table line draws over the 'number of under votes' text in SOVC report
9823 Revisited # 6774: Rotation Options dropdown menu displays duplicate entries in the Race Editor.

KCT 4.7.3 to 4.7.4
9687 The new name/type of the card reader (SecureTech ST-120) should be added to KCT
9996 KCT hangs if the ST-100 card reader is unplugged while creating/updating smart cards

ASS/ASM 1.2.1 to 1.2.2
10073 Allow users to specify database password at installation
10037 File is not deleted when the certificate store is closed
10038 File is not deleted when the certificate store is closed
9907 Display appropriate status message when fingerprint scan fails

PCS 2.2.1 to 2.2.2
10048 Eliminate repeated login entries in the Windows Event log
10036 File is not deleted when the certificate store is closed
10050 Unable to service upload requests when disk space is too low
10052 Going online multiple times with multiple hubs can result in deadlock
9872 Potential deadlock occurs when pruning old tally network hosts
9983 Remote ballot images not downloaded after delete and re-scan, or after some commit/rollback operations
9986 Excessively large clipping area displayed when viewing write-in report for landscape ballots

ANITIAN
ENTERPRISE SECURITY

APPENDIX B – CIS SECURITY TOOL REPORTS

This section contains the output of the CIS Security Tool, which was run against the final lab builds of the ASM, GEMS, PCS (running on a PS900) and the domain controller. Due to their large size, the reports are provided as four separate documents.